

Módulo IV: Guías Prácticas

Autores: Juan Carlos Caldera Palma
Wilberth Elieser Suazo Sequeira

Coordinador: Msc. Ing. Marlon Ramírez

INDICE

GUÍAS PRÁCTICAS DEL MÓDULO I: REDES DE TELEFONÍA1

LABORATORIO No. 1: INTRODUCCIÓN A LAS CENTRALES PBX *	3
LABORATORIO No. 2: CONFIGURACIÓN DE PBX DIGITAL PANASONIC MODELO KX-TD816SP. *	23
LABORATORIO No. 3: INSTALACIÓN DE PBX VIRTUAL *	33
LABORATORIO No. 4: CONFIGURACIÓN DE SERVICIOS EN PBX VIRTUAL	45
LABORATORIO No. 5: INTRODUCCIÓN AL MÓDULO EE-PM *	53
LABORATORIO No. 6: CODIFICACIÓN HDB3.....	61
LABORATORIO No. 7: RECEPCIÓN DE LA SEÑAL HDB3	67
LABORATORIO No. 8: SELECCIÓN DE RANURAS DE TIEMPO EN UNA LLAMADA TELEFÓNICA	71
LABORATORIO No. 9: FASES DE UNA CONEXIÓN TELEFÓNICA. *	77
LABORATORIO No. 10: TENSIONES Y SEÑALES DE CONTROL	87

GUÍAS PRÁCTICAS DEL MÓDULO II: REDES DE DATOS93

LABORATORIO No. 1: INTRODUCCIÓN AL SIMULADOR DE REDES.	94
LABORATORIO No. 2: INTRODUCCIÓN A WIRESHARK.....	107
LABORATORIO No. 3: EJERCICIOS INTRODUCTORIOS A REDES DE DATOS.....	117
LABORATORIO No. 4: DIRECCIONAMIENTO DE TRAMAS.....	125
LABORATORIO No. 5: PROTOCOLOS HDLC Y PPP.....	135
LABORATORIO No. 6: PROTOCOLO DE CAPA DE ENLACE FRAME-RELAY.	145
LABORATORIO No. 7: DIVISIÓN DE UNA RED EN SUBREDES USANDO VLSM.....	155
LABORATORIO No. 8: PROTOCOLOS IP, TCP Y UDP.....	161
LABORATORIO No. 9: PROTOCOLO DE ENRUTAMIENTO OSPF.	167
LABORATORIO No. 10: PROTOCOLOS ARP, ICMP, DHCP Y HTTP.....	177
LABORATORIO No. 11: INTRODUCCIÓN AL SIMULADOR DE RED GRAFICO GSN3.	183
LABORATORIO No. 12: PROTOCOLO DE CONMUTACIÓN POR ETIQUETA MPLS.....	203


GUÍAS PRÁCTICAS DEL MÓDULO III: TELEFONÍA IP217

LABORATORIO No. 1: CONFIGURACIÓN DE HIPATH 3000 VIA DTMF *	219
LABORATORIO No. 2: CONFIGURACIÓN DE HIPATH 3000 VIA SOFTWARE *	231
LABORATORIO No. 3: INTRODUCCIÓN A HIPATH 2000 *	255
LABORATORIO No. 4: CONFIGURACIÓN HIPATH 2000 Y ADAPTADOR ATA LINKSYS CISCO.....	267
LABORATORIO No. 5: ENLACE ENTRE HIPATH 2000 Y ASTERISK. *	289
LABORATORIO No. 6: ENLACE ENTRE HIPATH 2000 Y ASTERISK SOBRE MONITOREO. *	309
LABORATORIO No. 7: CONFIGURACIÓN DE CALL-CENTER EN ASTERISK	319
LABORATORIO No. 8: INTERCONEXIÓN DE CENTRALES ASTERISK A TRAVÉS DE RED MPLS.	337

¹ * Laboratorio tomado de la monografía titulada “Creacion de guias de laboratorio para la clase de redes telefonicas”.



Guías Prácticas del Módulo I: Redes de Telefonía





Laboratorio No. 1: Introducción a las centrales PBX *

Modulo	Redes de Telefonía		
Tipo Práctica	<input type="checkbox"/> Laboratorio <input type="checkbox"/> Simulación		
Unidad Temática			
No Alumnos por práctica	2	Fecha	
Nombre del Profesor			
Nombre(s) de Alumno(s)			
Tiempo estimado		Vo. Bo. Del Profesor	
Comentarios			

Objetivos de la práctica de laboratorio

I. Objetivo general

1. Familiar al estudiante con el entorno de las centrales telefónicas existentes en el laboratorio de Sistemas de Comunicaciones.

II. Objetivos específicos

1. Describir el contexto en el que se desarrollan las prácticas de laboratorio.
2. Presentar las características de las centrales privadas dentro del laboratorio de Sistemas de Comunicaciones.
3. Especificar los detalles técnicos de cada una de las centrales en estudio.

III. Medios a utilizar

- PBX Hipath 3000
- Teléfonos Siemens Optipoint 500 Standard
- PBX Hipath 2000
- PBX PANASONIC KX-TD816
- Equipo de cómputo

IV. Introducción

El entorno en el que vamos a trabajar se muestra en la figura 1:

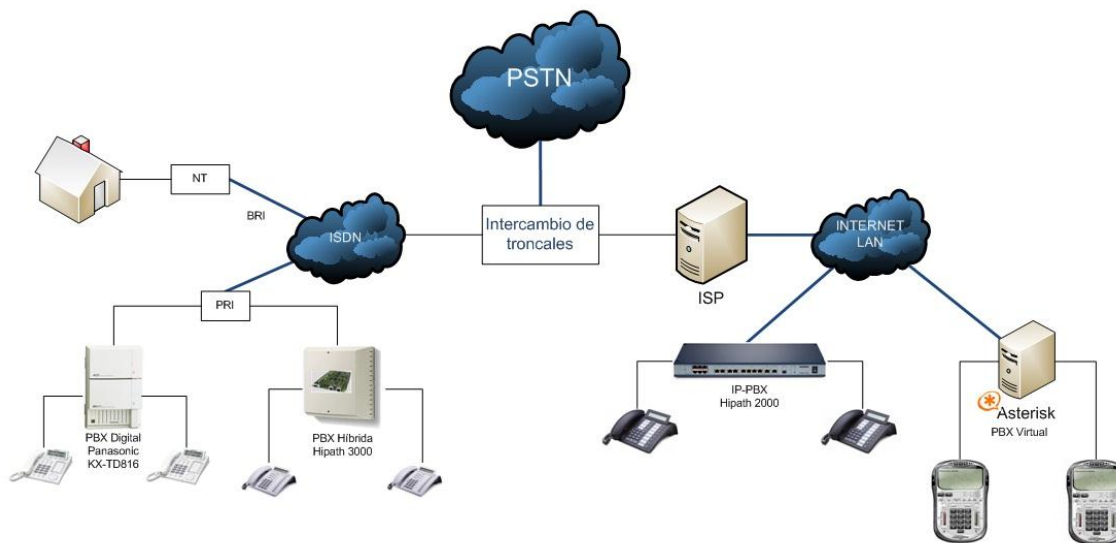


Fig. 1 Escenario de las centrales privadas PBX en el laboratorio

Esta práctica de laboratorio tiene como propósito dar a conocer a los estudiantes las centrales telefónicas con las que cuenta la universidad para realizar prácticas de laboratorio.

El laboratorio de sistemas de comunicaciones cuenta con 3 centrales telefónicas: 2 de la empresa Siemens y 1 de la empresa PANASONIC.

Además se cuenta con módulo práctico de transmisión y conmutación PCM que posee las características de una central digital de primer nivel o central local con la conexión de 4 teléfonos.

V. Conocimientos previos

- Central Privada o PBX (Private Branch eXchange).
- Servicios que brindan las PBX.

VI. Procedimiento

El procedimiento descrito a continuación es de carácter teórico. El brindará una descripción de las características que poseen las centrales en particular.

Tema 1: Central Hipath 2000

El sistema HiPath 2000 se presenta en tres variantes:

- HiPath 2020
- HiPath 2030
- HiPath 2036



Los datos técnicos se presentan a continuación:




Valores máximos	Hipath 2020 (rack 19")	Hipath 2030 (rack 19")	Hipath 2036 (rack 19")
			
Enlaces	2 S ₀ SIP (ISTP/WAN)	4 S ₀ SIP (ISTP/WAN)	6 a/b (CLIP)SIP (ISTP/WAN)
Extensiones analógicas	-	2	4
Extensiones IP	20	30	30
Extensiones totales	22	36	34
Wireless LAN (optiPoint WL2)	Sí	Sí	Sí
Puerto LAN Switch	4	4	4
Puerto DMZ	1	1	1
Puerto WAN	1	1	1
Puerto USB	1	1	1
DSP	8	8	8
EVM (Servidor vocal)	-	24 buzones	24 buzones
Gestión WEB (Acceso remoto vía LAN)	Sí	Sí	Sí
Dimensiones (Al x A x F) en mm	44,5x440x3801 U	44,5x440x3801 U	44,5x440x3801 U
Versión de software	V2.0	V2.0	V2.0

Tabla 1 Modelos de centrales Hipath 2000

Todas las centrales poseen las mismas magnitudes, iguales puertos LAN, 1 puerto WAN, 1 puerto USB y 1 puerto DMZ. La diferencia radica en las interfaces de intercambio, así como en las conexiones de líneas a/b para líneas subscriptoras.

El sistema Hipath 2020 posee 2 líneas S₀ mientras que la Hipath 2030 posee 4 líneas S₀ que se utilizan como configuración opcional ya sea como interfaz de intercambio o como interfaz de subscritor. La Hipath 2036 posee 6 puertos HKZ que se utilizan como troncales.



El modelo Hipath 2000 posee una dirección gateway que funciona como el interfaz entre la LAN/WAN y los circuitos de intercambio tradicionales. Esta dirección gateway por defecto es la 192.168.1.2 modificable mediante administración. La asignación de números de telefonía IP facilita el movimiento de los empleados y los lugares de trabajo.

La administración de la central Hipath 2000 se realiza vía Web conocido como WBM, introduciendo la dirección IP determinada en el explorador de preferencia. Aquí se pueden realizar las modificaciones de los parámetros y configuraciones entrando en un llamado “Modo experto”.

Escenario general de la central Hipath 2036

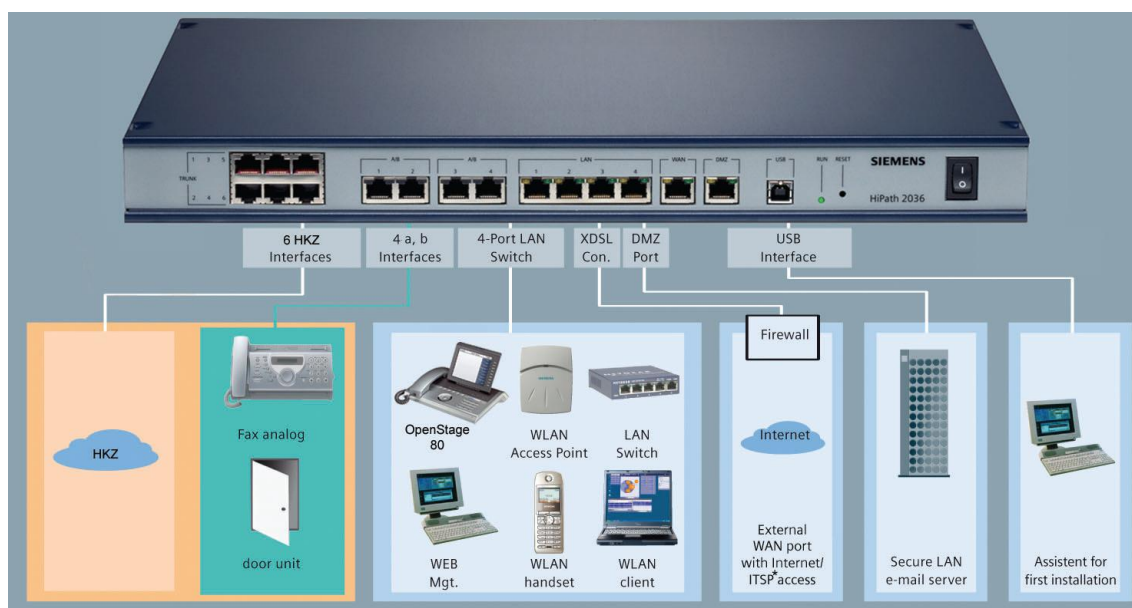


Fig. 2 Escenario de Hipath 2000

HiPath 2036 ofrece una amplia gama de opciones de conexión, tanto para la red telefónica pública como el lado del usuario. La conexión de circuitos de intercambio tradicionales se pueden utilizar en paralelo con las conexiones a proveedores de servicios de telefonía de Internet (ISP / ITSP).

Se pueden utilizar como terminales teléfonos analógicos convencionales o dispositivos tales como máquinas de fax y apertura de puertas. Además pueden emplearse adaptadores analógicos adicionales.

Todos los tipos de dispositivos IP se pueden conectar a la interfaz LAN a través del switch externo, el cual también suministra la energía necesaria a estos



dispositivos (Power-over-Ethernet). En combinación con estaciones base WLAN adicionales es posible la comunicación inalámbrica tanto para aplicaciones de voz y datos, por ejemplo, utilizando un teléfono WLAN o un optiClient 130 instalado en una portátil.

La interfaz de Internet para comunicaciones de voz y datos están protegidos por un firewall.

Se puede configurar un servidor de correo electrónico en el puerto DMZ, aislado del resto de la infraestructura interna de la empresa, para la transmisión de entrada de correo electrónico a su respectivo destinatario.

La interfaz USB se utiliza para la configuración inicial del sistema.






Tema 2: Central Hipath 3000

El sistema Hipath 3000 presenta las siguientes variantes:

- HiPath 3750/3700
- HiPath 3550/3500
- HiPath 3350/3300

El modelo Hipath 3750 es un sistema montado sobre el suelo, mientras que las variantes 3550 y 3350 son sistemas montado en pared. Los Rack de 19" corresponden a los modelos Hipath 3700 donde los periféricos se conectan en un patch panel y a los modelos 3500/3300 donde los periféricos se conectan directamente a la terminal RJ-45.

La variante presentada en este documento es el montado sobre pared correspondiente a la Hipath 3550 con el cual se presentan los diseños de algunos laboratorios.

Valores máximos	Hipath 3300 (rack 19")	Hipath 3350 (sist. mural)	Hipath 3500 (rack 19")	Hipath 3550 (sist. mural)	Hipath 3800 (suelo o rack 19")
					
Extensiones analógicas	20	36	44	96	384
Extensiones digitales	24	24	48	72	384
Extensiones	96	96	192	192	500



IP					
Extensiones inalámbricas	16	16	32	64/32	250
Estaciones base de Hipath Cordless Office	3	3	7	16/7	64
Interfaces V.24	1	2	1	2	2
optiClient Attendant (Operadora en PC)	4	4	4	4	6
Número de enlaces	16	16	60	60	250
Número de canales B	16	16	60	60	180
Enlaces IP	16	16	48	48	128
Nodos de red IP en LAN	32	32	32	32	32
Módulos HG1500	1	1	3	3	8
Dimensiones (Al x A x F) en mm	89x440x3802 U	450x460x130	155x440x3803,5 U	450x460x200	490x410x390
Versión de software	V7.0	V7.0	V7.0	V7.0	V7.0
Peso	Aprox. 6 Kg	Aprox. 6 Kg	Aprox. 8 Kg	Aprox. 8 Kg	16,5 Kg base 15 Kg expansión
Color de la caja	Verde azul	Gris claro	Verde azul	Gris claro	Azul metal

Tabla 2 Especificaciones de la Familia Hipath 3000.

La central Hipath 3000 se puede administrar vía DTMF mediante teléfonos propietarios como el Optipoint 500 Standard.



Fig. 3 Optipoint 500 Standard

En este tipo de administración el teléfono posee un panel de control que facilita la movilidad en las opciones que se desean programar. Para iniciar el modo de programación basta ingresar el comando *95 e introducir el nombre de usuario y contraseña del sistema que por defecto es 31994. Luego aparecerán las prestaciones o servicios que dispone la central que se pueden modificar.

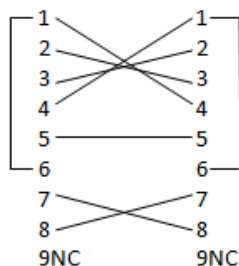
Asimismo la central también se puede manipular mediante una aplicación para PC. El software de administración para el sistema de comunicación Hipath 3000 es el HiPath 3000 Manager E. Es una herramienta de servicio que se ejecuta bajo Microsoft® Windows en un PC conectado al sistema vía V.24, S₀ o interfaz LAN basado en TCP-IP.

Para hacer la conexión de la PC con la central para la transmisión de la información a través del software se utiliza un cable serial con terminales RS232 de 9 pines. La configuración que posee dicho cable es utilizada únicamente por las centrales Siemens.

El tipo de conexión que se utiliza para la configuración del cable RS232 se muestra en la figura 4:

Cable de HIPATH 3000

DB9 (Hembra) DB9 (Hembra)



Cable HIPATH 3750

DB9 (Hembra) DB25 (Macho)

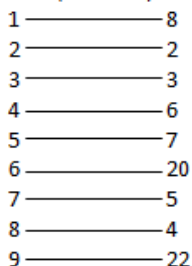


Fig. 4 Cable RS232 para la Central Hipath 3000

El software Hipath 3000 Manager E se instala en el ordenador de forma que facilita la administración de la central telefónica. A través del Hipath 3000 Manager E se realizan las mismas configuraciones que en DTMF, la diferencia es que se tiene un interfaz más agradable para la persona que está realizando la configuración.

La principal ventaja acerca del Manager E es que se puede descargar un archivo de base de datos KDS y modificarlo tantas veces como quiera sin cambiar el sistema en caliente, o sea mientras esté trabajando.

Se debe descargar una KDS antes de hacer cualquier trabajo, o bien cargar una KDS guardada, hacer los cambios y luego realizar la transferencia de nuevo al sistema. Si algo sale mal sólo puede cargar la KDS original que se tenía guardada.

Escenario general de la central Hipath 3550

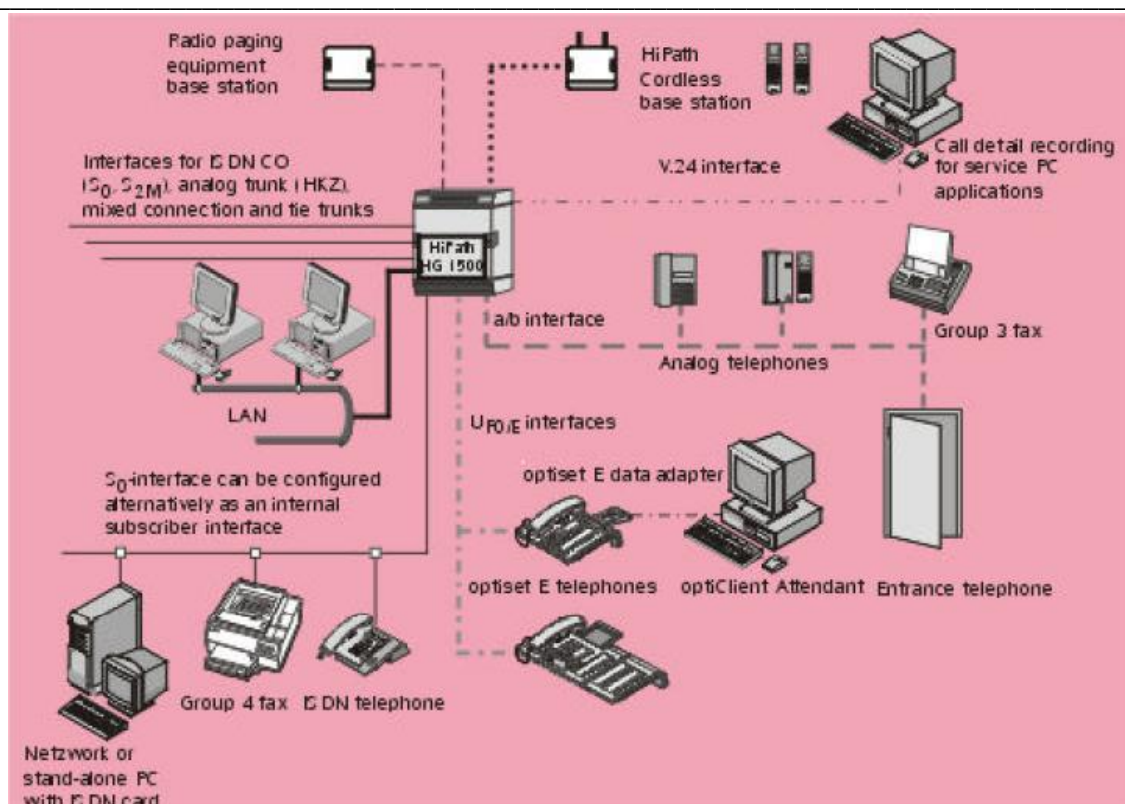


Fig. 5 Escenario de HiPath 3000

La figura 5 muestra un esquema de interconexión de la HiPath 3550.

Las terminales a/b se utilizan para conectar teléfonos estándar y terminales analógicos como fax de grupo 2 y 3, módem, contestadores, entre otros.

La interfaz $U_{P0/E}$ es de tipo digital para conectar teléfonos Optiset E, Optipoint 500 a dos hilos, estaciones base DECT (Digital Enhanced Cordless Telecommunications).

El puerto V.24 se emplea para conectar una PC de servicio, tarifador o una impresora para registrar todos los detalles de las llamadas.

Las interfaces s_0 son útiles para conexión digital dedicada ya sea a troncales ISDN o a terminales ISDN (teléfonos ISDN, dispositivo fax del grupo 4, PC).

Con el módulo HiPath HG 1500, la conexión de las plataformas de comunicaciones HiPath 3000 se realiza vía LAN Ethernet.



HiPath HG 1500 convierte el sistema HiPath en un servidor de comunicaciones de voz, datos y vídeo que cubre todos los requisitos aplicables para pequeños y medianos niveles de tráfico de datos.

Tema 3: PANASONIC KX-TD816

Es una centralita híbrida para 4 líneas y 8 extensiones híbridas, ampliables a 8 líneas y 16 extensiones.

KX-TD816	Sistema básico	Con unidades opcionales	Conexión de sistema
Línea Exterior	4	8	-
Extensión	8	16	-

Tabla 3 Especificaciones Panasonic KX-TD816

Este sistema puede doblar la capacidad de extensiones conectando un teléfono específico y un teléfono de línea única. El teléfono específico puede compartir la extensión con otro teléfono de línea única. Además, puede conectar un teléfono específico digital Panasonic y un teléfono de línea única a un conector y utilizarlos como extensiones individuales.

La administración de esta central híbrida se puede realizar mediante DTMF. Se pueden utilizar teléfonos regulares, como un teléfono de impulsos o un teléfono específico Panasonic como el KX-T7533 a utilizarse en el laboratorio junto con el KX-TS3EX.



Fig. 6 Teléfonos específicos PANASONIC: a) KX-T7533; b) KX-TS3EX

Asimismo existe un software de aplicación E1232B2 para la administración de la central en el entorno MS-DOS. Esta programación es posible conectando la PC a través de un puerto serie para obtener los datos de la central para su administración.

Este tipo de administración presenta las ventajas de imprimir y salvar datos, visualizar en la pantalla del monitor información relativa a situaciones, etc. Para ello es suficiente conectar el cable de comunicaciones suministrado entre un



puerto serie del PC y el terminal RS-232 de la central dispuesto en el lateral derecho.

Escenario general de la central Panasonic KX-TD816

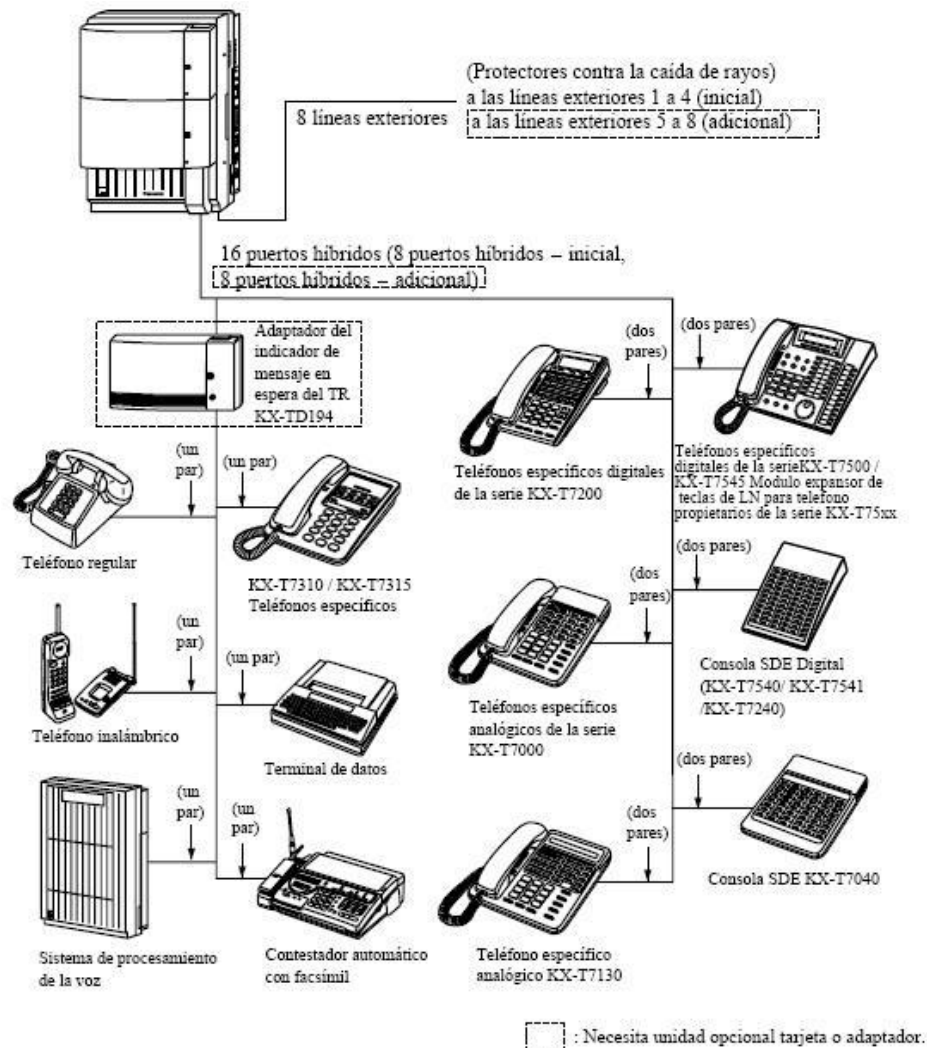


Fig. 7 Escenario de la central KX-TD816

En la figura 7 se presenta un diagrama acerca de las conexiones de líneas troncales y extensiones que se pueden realizar con la central Panasonic KX-TD816. Aquí se muestran los dispositivos terminales que se pueden conectar a las extensiones.

Características Técnicas

Método de control	CPU: CPU de 16 bits
Conmutación	Conmutador de tiempo PCM sin



		bloqueo
Alimentaciones	Primaria	KX-TD816: 220 VCA – 230 VCA, 50 Hz / 60 Hz KX-TD1232: 220 VCA – 240 VCA, 50 Hz / 60 Hz
	Secundaria	Alimentación de la extensión: 30 V Voltios del circuito: ± 5 V, ± 15 V
	Fallo en la alimentación	<ul style="list-style-type: none">• Duración de la memoria de seguridad: siete años con la batería de litio suministrada• 4 líneas exteriores como máximo para el modelo KX-TD816, y 6 líneas exteriores como máximo para el modelo KX-TD1232 asignadas automáticamente a las extensiones (fallo de alimentación)• Funcionamiento del sistema durante unos diez minutos con la batería de seguridad opcional y la tarjeta adaptadora (KX-A216) para el KX-TD816.• Funcionamiento del sistema durante unas tres horas utilizando las baterías recomendadas (dos baterías de 12VCC.)
Marcación	Externa	Marcación por pulsos (DP) 10 pps, 20 pps Marcación por tonos (DTMF)
	Interna	Marcación por pulsos (DP) 10 pps, 20 pps Marcación por tonos (DTMF)
Conectores	Líneas exteriores	Conector modular
	Extensiones	KX-TD816: Conector modular KX-TD1232: Conector Amphenol
	Salida de búsqueda	Conector de patillas (CONECTOR RCA)
	Entrada de música externa	Dos conectores conductores (MINI CONECTOR de 3,5 mm de diámetro)



Límite de bucle de extensión	Teléfono específico: 40 Ω Teléfono regular: 600 Ω incluido el grupo Interfono: 20 Ω
Mínima resistencia a la pérdida	15000 Ω
Máximo número de extensiones por puerto híbrido	<ul style="list-style-type: none">➤ 1 para teléfono específico o teléfono regular➤ 2 en paralelo o mediante conexión de puerto de dispositivo extra de un teléfono específico y un teléfono regular.
Voltaje de llamada	70 Vrms a 25 Hz, según la carga de llamada
Límite de bucle de la red telefónica	1600 Ω máx.
Requisitos de entorno	0 °C – 40 °C, 10 % – 90 % humedad relativa
Rango del tipo de Flash de gancho de colgar	204 ms – 1000 ms

Tabla 4 Datos Técnicos de la central Panasonic KX-TD816

Tema 4: Central Asterisk

Asterisk es un programa de software libre que provee de una gran cantidad de funcionalidades que posee una central telefónica (PBX) como las mencionadas anteriormente. Como cualquier PBX, se puede conectar un número determinado de teléfonos para hacer llamadas entre sí e incluso conectar a un proveedor de VoIP o bien a una ISDN tanto básicos como primarios.

Las centrales Asterisk se montan a partir de una PC, corriendo un software determinado. Se trata de una central que opera completamente en VoIP.

Para la administración se utilizan las herramientas Web del servidor (la computadora donde se instala el Asterisk) o través de la interfaz de comandos del Trixbox en LinuxCentos, basado en Linux Red Hat Enterprise el cual se compone de software libre y código abierto.

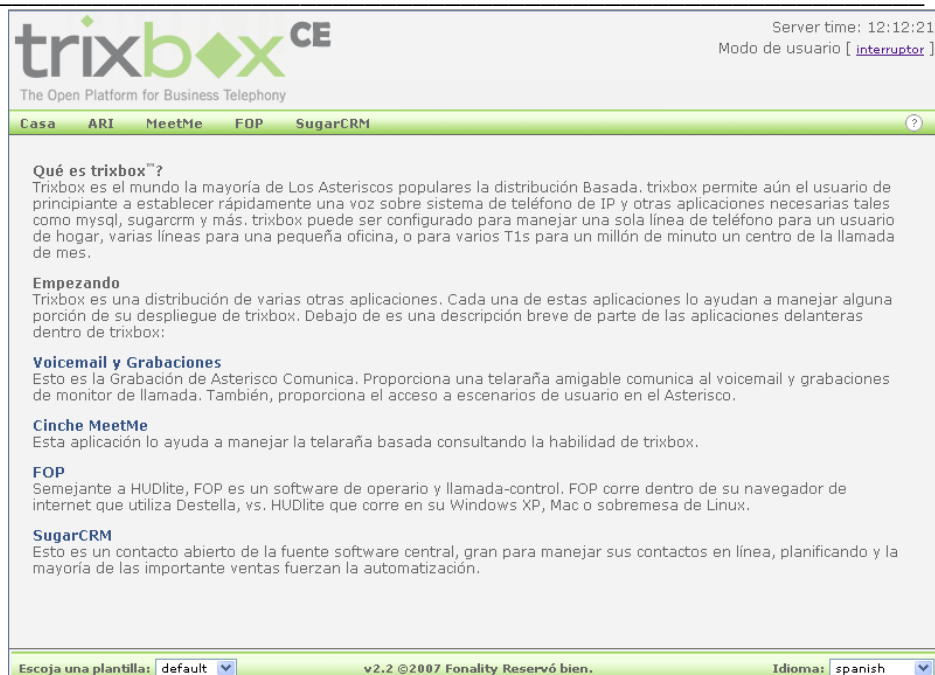


Fig. 8 Administración web de Asterisk

Tema 5: Módulo PCM/EV

El módulo PCM/EV (Pulse-Code Modulation/Electronic Veneta) es un equipo de Telefonía Fija, constituido por módulos experimentales, entrenadores y demás equipos que permiten el desarrollo de cursos teórico-experimentales para el estudio de todas las nociones, los aparatos y los sistemas utilizados en la telefonía moderna.

Es un sistema que permite analizar todos los principales aspectos correspondientes a la codificación, la conmutación y la transmisión digital de señales PCM.

Desarrolla las funciones típicas de una central telefónica y un sistema Multiplex PCM de primer nivel 2.048kbps-32 canales, utilizado para la transmisión simultánea de varios canales telefónicos a distancia, completo también de la sección de recepción necesaria.

El sistema PCM/EV está constituido por los siguientes componentes:

- Interfaz con las líneas de usuario.
- Unidad de conmutación digital.
- Interfaz con la línea externa.
- Línea simulada.



-
- Receptor de línea.
 - Transmisor de línea.
 - Base de tiempos.
 - Generador de tonos.

Interfaz con las líneas de usuarios:

Esta sección convierte las señales analógicas de fonía en secuencias binarias multiplexadas en un bus PCM a cuatro hilos. Se compone de:

- El interfaz de usuario propiamente dicho SLIC (Subscriber Line Interface Circuit).
- Los circuitos de codificación y decodificación PCM de las señales de fonía (CODEC).
- Los circuitos de acceso a las multiplexaciones PCM de las fonías de recepción y transmisión.

En el teléfono a multifrecuencia está presente también el circuito de decodificación de los tonos de servicio, colocado inmediatamente después de la interfaz de usuario.

Unidad de conmutación digital:

Esta unidad se encuentra entre:

- La multiplexación PCM conectada a las líneas de usuario.
- La multiplexación PCM que procede de la línea externa (sistema primario).

En la unidad de conmutación digital se realizan las asignaciones de espacio y tiempo que instauran los circuitos de fonía entre los canales PCM.

Interfaz con la línea externa:

El interfaz se halla en un único circuito integrado, que realiza la función de intermediario entre las señalizaciones bipolares (HDB3) de la línea externa, organizadas según el esquema primario CEPT.

Transmisor de línea (BIPOLAR LINE DRIVER):

El transmisor de línea tiene la función de introducir en la línea externa las señalizaciones bipolares transmitidas por el interfaz CEPT.

Línea externa (LINE):



La línea externa es simulada por una red que introduce la atenuación y las distorsiones típicas de los pares balanceados. En la línea simulada se introduce también un nivel regulable de ruido (NOISE GENERATOR).

Receptor de línea:

El receptor de línea transfiere al interfaz CEPT las señalizaciones bipolares de recepción de la línea externa. Incluye el ecualizador de línea (LINE EQUALIZER) el cual elimina las componentes de frecuencias indeseables, el regenerador de reloj (CLOCK RECOVERY) un circuito que coincide con el tiempo de la señal original y el detector de datos (DATA DETECTOR) que determina si fue enviado un 0 o un 1.

Base de los tiempos (PCM TIMING):

Este circuito extrae, de un oscilador de cristal de cuarzo a 4096 Hz, las señales de sincronismo, bit y trama, que suministran el control temporal de las multiplexaciones PCM en división de tiempo.

Generador de los tonos (TONES GENERATOR):

Genera y temporiza los tonos de señalización de la central. Cuando un usuario quiere llamar, la central envía un “tono de marcado” que tiene una frecuencia de 425 Hz, para la persona que llama para así indicar que una línea está disponible. El tono de marcado está modulado ON/OFF en secuencia TONO/PAUSA/TONO/PAUSA. Una vez que se recibe el número marcado, la central lleva a cabo la conexión y envía el tono libre a la persona que llama. Este tono también tiene una frecuencia de 425 Hz y se modula ON/OFF = TONO/PAUSA con una razón de 1s/4s. Si la persona llamada está ocupada, la central envía TONO DE OCUPADO, la cual es una secuencia alterna de TONO/PAUSA de igual duración y período equivalente a 1s.

Unidad de control (μ P):

La gestión de las conexiones que entran en acción por el sistema es confiada a una unidad de control (μ P) provista de microprocesador; la misma unidad realiza también otras funciones, por ejemplo:

- Programar las funciones de los circuitos PCM (CODECS) asignando, entre otras, los intervalos temporales (time slot) de recepción y transmisión a los distintos teléfonos.



- Interceptar las señalizaciones de servicio producidas por los terminales de usuario y transmitir a los mismos las señalizaciones de servicio emitidas por la central.
- Programar las funciones del interfaz CEPT recibiendo del mismo las señalizaciones de alarma y de estado.

Para estas funciones la unidad de control se vale de:

- Un puerto de uso general puesto a disposición por los “CODECS”
- Tres líneas en serie multiplexadas de la matriz de conmutación, programables para la transferencia de los datos (en lugar de las señalizaciones PCM)

La unidad de control está conectada también en RS232 con un ordenador personal, que puede asumir la función de supervisor de las actividades desarrolladas.

Características Técnicas

- 4 Interfaces de usuario (SLIC) para la conexión de 4 teléfonos:
 - 3 con marcación por impulsos (PULSE)
 - 1 con marcación multifrecuencia (DTMF)
- 4 CODECs que ejecutan para cada usuario las siguientes funciones:
 - Filtrado
 - Conversión en PCM de la señal fónica y viceversa.
 - Asignación de los time-slots.
 - Formación de la trama serie de 32 canales (2.048 kb/s).
- 1 Matriz de conmutación digital que “encamina” las señales PCM para realizar las conexiones requeridas.
- 1 Microprocesador de gestión, interfazable con PC, para operaciones de supervisión y programación de los parámetros de funcionamiento de la central.
- 1 Interfaz CEPT que permite simular la conexión con otra central telefónica e incluye:
 - Codificador-transmisor HDB3
 - Ecualizador de línea
 - Regenerador del reloj de recepción
 - Receptor-decodificador HDB3
- 1 Línea artificial



- 1 Generador de ruido
- 1 Sistema de sincronización para la visualización en el osciloscopio de los time slots
- Estructura: caja de soporte compacta con tapa que se puede alzar; incorpora todas las partes electrónicas, los puntos de medida y el simulador de averías; la tapa incluye el diagrama de bloques del circuito y los LEDS de señalización.
- Puntos de medida: 34 montados en circuito impreso, y conectados directamente a los circuitos del equipo
- Simulador de averías: 12 averías activables por medio de interruptores, protegido mediante tapa con cierre de llave
- Alimentación: 230Vac (110Vac bajo pedido) – 50/60 Hz
- Dimensiones: 420x130x360 mm (cerrado)

Actividad 1: Diseño

1. Diseñar el cable DB9 para las configuraciones de software mediante la interfaz V.24 procedente de la central Hipath 3000.

VII. Preguntas de control

1. ¿Qué es una central IP?
2. ¿Qué es una central virtual?
3. ¿Para qué se utilizan las interfaces S_0 en las centrales Siemens?
4. ¿Es posible ampliar el número de extensiones que trae por defecto la central Hipath 2036? ¿Por qué?
5. ¿Es posible ampliar el número de extensiones que trae por defecto la central Hipath 3550? ¿Por qué?
6. ¿Es posible ampliar el número de extensiones que trae por defecto la central Panasonic KX-TD816? ¿Por qué?
7. ¿Qué función tienen los puertos HKZ en la central Hipath 2036?
8. ¿Se pueden conectar teléfonos en paralelo en la Central Panasonic KX-TD816? ¿Por qué?



-
9. Enliste al menos 5 módulos adicionales con sus características que se pueden agregar en la central Hipath 3550.
 10. ¿Cuáles son las ventajas que posee el servidor Asterisk sobre las centrales convencionales?
 11. ¿Cuáles son las desventajas que posee el servidor Asterisk sobre las centrales convencionales?
 12. ¿Para qué se utiliza el módulo PCM/EV?

VIII. Bibliografía

1. Manual de la central Hipath 2000
2. Manual de la central Hipath 3000
3. Manual de la central Panasonic KX-TD816
4. Manual del módulo PCM/EV
5. Asterisk desconsolidado
6. Asterisk al descubierto



Laboratorio No. 2: Configuración de PBX digital Panasonic modelo KX-TD816SP. *

Modulo	Redes de Telefonía		
Tipo Práctica	<input type="checkbox"/> Laboratorio <input type="checkbox"/> Simulación		
Unidad Temática			
No Alumnos por práctica	2	Fecha	
Nombre del Profesor			
Nombre(s) de Alumno(s)			
Tiempo estimado		Vo. Bo. Del Profesor	
Comentarios			

Objetivos de la práctica de laboratorio

I. Objetivo general

1. Programar configuraciones básicas en la PBX analógica Panasonic modelo KX-TD816SP.

II. Objetivos específicos

1. Configurar extensiones telefónicas.
2. Asignar servicios básicos en la PBX analógica Panasonic modelo KX-TD816SP.

III. Medios a utilizar

- PBX analógica Panasonic modelo KX-TD816SP.
- 2 Teléfonos Panasonic KX-T7533.
- 1 Teléfono Panasonic KX-TS3EX.

IV. Introducción

La central telefónica Panasonic modelo KX-TD816SP tiene 4 líneas exteriores a su sistema y 8 número de extensiones con unidades opcionales de 8y16 respectivamente. De ahí debe su nombre KX-TD816SP. Existe un software de aplicación E1232B2 para la administración de la central en el entorno MS-DOS. Esta programación es posible conectando la PC a través de un puerto serie para obtener los datos de la central para su administración.

Este tipo de administración presenta las ventajas de imprimir y salvar datos, visualizar en la pantalla del monitor información relativa a situaciones, etc. Para ello es suficiente conectar el cable de comunicaciones suministrado entre un puerto serie del PC y el terminal RS-232 de la central dispuesto en el lateral derecho.

En esta práctica se efectúa la configuración de la central vía DTMF utilizando el teléfono propietario PANASONIC conocido como KX-T7533. Se realiza la configuración de la fecha del sistema, se hacen cambios en las configuraciones de los nombres y números de las extensiones.

También se programan servicios en teclas de funciones flexibles que ya hayan sido o no asignadas anteriormente. Finalmente se efectúa una transferencia de llamada y se establece una conferencia entre las extensiones disponibles.

En esta central se pueden utilizar teléfonos regulares, como un teléfono de impulsos o un teléfono específico Panasonic como el KX-T7533 a utilizarse en el laboratorio junto con el KX-TS3EX.

A continuación se presenta la ubicación y nombre de las teclas:

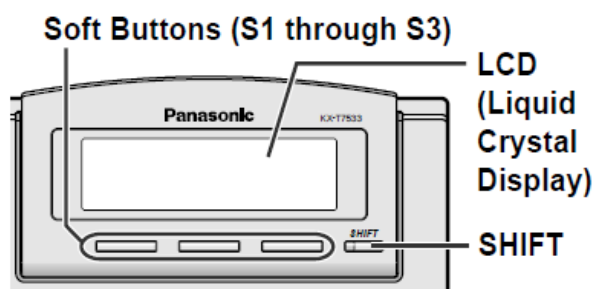


Fig. 1 Pantalla del modelo de teléfono Panasonic KX-T7533

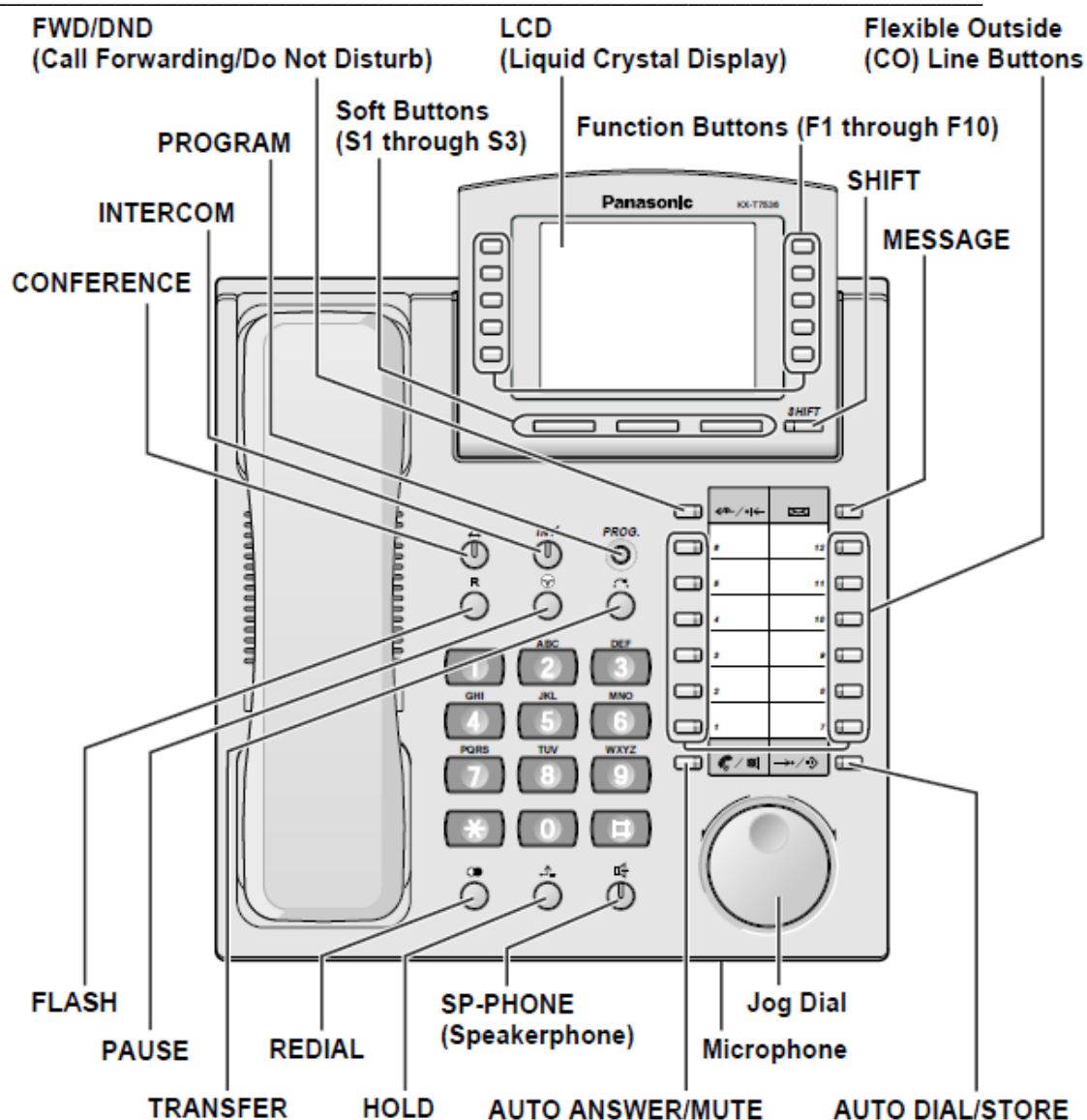


Fig. 2 Modelo de teléfono Panasonic KX-T7536

La parte de la pantalla del KX-T7533 es la correspondiente a la figura 1.

En este laboratorio se pretende hacer programación general a pequeña escala, involucrando fecha y hora, números y nombres de extensiones, programación de teclas, entre otros.

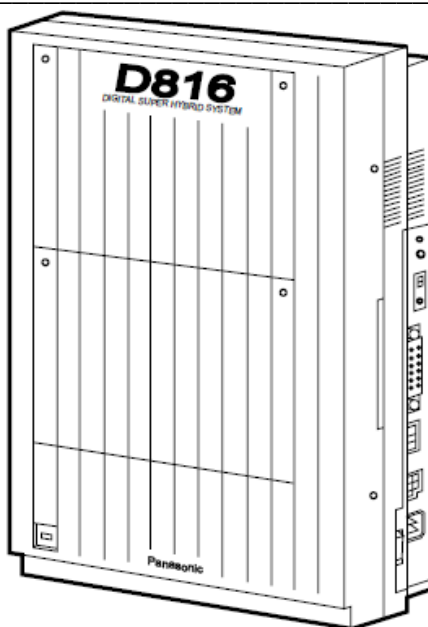


Fig. 3 Central Panasonic modelo KX-TD816SP.

V. Conocimientos previos

- Diagrama del hardware de la central Panasonic modelo KX-TD816SP
- Diagrama del teléfono Panasonic KX-T7536
- Central Privada o PBX (Private Branch eXchange).
- Servicios que brindan las PBX.

VI. Procedimiento

El escenario a implantarse se muestra en la figura 4. Aquí se presentan los medios a utilizar como son la centralita Panasonic modelo KX-TD816SP y los Teléfonos Panasonic KX-T7533 y KX-TS3EX:



Fig. 4 Escenario del laboratorio

Actividad 1: Conexión

1. Conecte la central Panasonic al suministro eléctrico (220 V) y oprima el switch de encendido/apagado.
2. Conecte los teléfonos propietarios Panasonic a las terminales de extensiones del panel que contiene la central, distribuidos de la siguiente manera: en el puerto 01 y 02 modelo de teléfono KX-T7533 y en el puerto 03 el modelo de teléfono KX-TS3EX.

Actividad 2: Programación

1. Acérquese al teléfono que se encuentra conectado a la primera terminal de extensión.
2. Presione la tecla prog e ingrese el código *#1234 para entrar al modo de programación del teléfono.

Actividad 2.1: Modificar fecha del teléfono

1. Estando en el modo de programación del teléfono ingrese el código 000. Inmediatamente aparecerá en la pantalla del teléfono Graba FECHA/HORA.
2. Presione siguiente y a continuación aparecerá el formato de fecha: Año/Mes/Día/Nombre del día.
3. Ingrese el año y si ya hay una fecha existente presione borrar e ingréselo nuevamente.
4. Presione la flecha direccional → para cruzar al siguiente dato, el cual corresponde al mes. Presione select hasta que aparezca el mes correcto.
5. Pulse nuevamente la flecha direccional → para cruzar al dato siguiente, es decir el día



6. Ingrese el número correspondiente al día y si ya hay un número existente presione borrar e ingréselo nuevamente.
7. Pulse flecha direccional → para pasar al dato siguiente correspondiente al día de la semana.
8. Presione select hasta que aparezca el día correcto.
9. Una vez que ya se ingresaron todos los datos presione memoria para que los cambios queden guardados.

Actividad 2.2: Modificar los números de extensiones del teléfono

1. Estando en el modo de programación del teléfono ingrese el código 003. Inmediatamente aparecerá en la pantalla del teléfono GRABA NUMERO DE EXTENSIÓN.
2. Presione sigue. En la pantalla aparecerá CONCTR NO, esto corresponde al número de conector. Nota: Existen 16 conectores cada uno con la capacidad de conectar dos teléfonos.
3. Presione sigue para buscar el número del conector del teléfono al cual desea modificar el número de extensión.
4. Una vez situado en el conector deseado marque el número que quiere asignar a la extensión.
5. Presione la tecla Memoria.

Actividad 2.3: Modificar los nombres de las extensiones del teléfono

1. Estando en el modo de programación del teléfono ingrese el código 003. Inmediatamente aparecerá en la pantalla del teléfono GRABA NUMERO DE EXTENSIÓN.
2. Presione sigue. En la pantalla aparecerá CONCTR NO, esto corresponde al número de conector. Nota: Existen 16 conectores cada uno con la capacidad de conectar dos teléfonos.
3. Presione sigue para buscar el número del conector del teléfono al cual desea modificar el número de extensión.
4. Una vez situado en el conector deseado marque el número que quiere asignar a la extensión.
5. Presione la tecla Memoria.


Actividad 2.4: Programación de teclas LN flexibles

1. Estando en el modo de programación del teléfono ingrese el código 005. Inmediatamente aparecerá en la pantalla del teléfono ASIG TECL FLEX.
2. Presione sigue. En la pantalla aparecerá CONCTR NO, esto corresponde al número de conector. Nota: Existen 16 conectores cada uno con la capacidad de conectar dos teléfonos.





3. Presione sigue y a continuación aparecerá en la pantalla MODO PROG TLESPF, permitiéndole programar las teclas flexibles.
4. Marque la tecla flexible que desea programar, notará que aparece en la pantalla el número de la tecla flexible, ej. LN-01 o bien la función que haya sido programada anteriormente en dicha tecla.
5. Posteriormente ingrese un código de la tecla correspondiente a la función que se desea programar en la tecla flexible, más parámetro de ser necesario. Para ayuda de código tecla vea la tabla 2 en anexos.
6. Presione la tecla Memoria.

Actividad 3: Transferencia de llamadas

1. Para la transferencia de llamadas puede optar por dos opciones:
2. Para cualquier modelo de teléfono Panasonic. Al recibir una llamada pulse suavemente colgar y luego marque la extensión a la cual se desea transferir la llamada y posteriormente cuelgue el teléfono.
3. Para el modelo Panasonic KX-T7533 puede habilitar simplemente la tecla  que corresponde a transferir, luego marque la extensión deseada y cuelgue el teléfono.

Actividad 4: Conferencia de llamadas

1. Para la conferencia de llamadas puede optar por dos opciones:
2. Para cualquier modelo de teléfono Panasonic. Al estar en medio de una llamada pulse suavemente colgar y luego marque la extensión con la cual desea realizar la conferencia y posteriormente vuelva a presionar levemente colgar y marque 3.
3. Para el modelo Panasonic KX-T7533 al estar en medio de una llamada pulse la tecla  que corresponde a conferencia y luego marque la extensión deseada y luego vuelva a pulsar .

Actividad 5: Asignación

1. Modifique la hora del teléfono siguiendo las indicaciones de la actividad 2.1.
2. Programe un mensaje de ausencia en el modo de programación digitando 008.
3. Escriba el procedimiento utilizado para programar la hora del teléfono y el mensaje de ausencia.

VII. Orientaciones del reporte de laboratorio

Adjunte el diagrama del hardware de la central Panasonic modelo KX-TD816SP



Adjunte el diagrama del teléfono Panasonic KX-T7536

Se deberá seguir el formato de informes de laboratorios. Además se deben presentar las respuestas de las preguntas de control.

VIII. Bibliografía

1. Panasonic. (1999). Sistema Súper Híbrido Digital.

<http://www.ferpa.es/html/centralitas/soporte%20cliente/KX-TD816%20Usuario.pdf>

IX. Anexos

Tecla Soft		S1	SHIFT+S1	S2	SHIFT+S2	S3	SHIFT+S3	SHIFT+SHIFT+S1	SHIFT+SHIFT+S2
Pulsaciones de la tecla SELECT	0	1	2	3	4	5	6	7	8
teclas									
1	1	Q	q	Z	z	!	?		
2	2	A	a	B	b	C	c		
3	3	D	d	E	e	F	f		
4	4	G	g	H	h	I	i		
5	5	J	j	K	k	L	l		
6	6	M	m	N	n	O	o		
7	7	P	p	Q	q	R	r	S	s
8	8	T	t	U	u	V	v		
9	9	W	w	X	x	Y	y	Z	z
0	0	(espacio)	.	,	'	:	;		
*	*	/	+	-	=	<	>		
#	#	\$	%	&	@	()		

Fig. 5 Tabla de valores para introducir caracteres



Código de tecla	Parámetro
0 (Única-LN)	KX-TD816: de 01 a 08 (Número de línea exterior) KX-TD1232: de 01 a 54 (Número de línea exterior)
1 (SDE)	de 2 a 4 dígitos (Número de extensión)
2 (Marcación con una sola pulsación)	máx. 16 dígitos (p.ej. Número de teléfono)
3 (Mensaje en espera)	Ninguno
3 (Mensaje en espera en otra extensión)	de 2 a 4 dígitos (Número de otra extensión)
3 (Mensaje en espera en extensión virtual)	de 2 a 4 dígitos (Número de extensión virtual)
4 (DSV/NOM)	Ninguno
5 (Guardar)	Ninguno
6 (Cuenta)	Ninguno
70 (Conferencia)	Ninguno
71 (Registro/Baja)	Ninguno
72 (Extensión virtual)	de 2 a 4 dígitos (Número de extensión virtual)
73 (Noche)	Ninguno
8 (Transferencia de correo vocal)	de 2 a 4 dígitos (Número de extensión de correo vocal)
90 (Grabación de conversaciones)*	de 2 a 4 dígitos (Número de extensión de correo vocal)
91 (Grabación de conversaciones en buzón ajeno)*	de 2 a 4 dígitos (Número de extensión de correo vocal)
92 (Monitorización de correo vocal)*	Ninguno
93 (Cancelar monitorización de correo vocal)*	Ninguno
* (Bucle-LN)	Ninguno
# (Grupo-LN)	de 1 a 8 (Número de grupo de línea externa)
LN (Frecuencia de timbre)	de 1 a 8 (Número de tipos de tono de timbre)

Fig. 6 Programación de teclas LN flexibles





Laboratorio No. 3: Instalación de PBX virtual *

Modulo	Redes de Telefonía		
Tipo Práctica	<input type="checkbox"/> Laboratorio <input type="checkbox"/> Simulación		
Unidad Temática			
No Alumnos por práctica	2	Fecha	
Nombre del Profesor			
Nombre(s) de Alumno(s)			
Tiempo estimado		Vo. Bo. Del Profesor	
Comentarios			

Objetivos de la práctica de laboratorio

I. Objetivo general

1. Configurar el servidor Asterisk mediante interfaz web.

II. Objetivos específicos

1. Instalar el servidor Asterisk a través de una máquina virtual.
2. Añadir extensiones SIP.
3. Establecer la comunicación entre softphones.

III. Medios a utilizar

- Equipo de cómputo
- Router o Switch
- Disco de instalación de Trixbox
- Softphone Zoiper o Xlite

IV. Introducción

Asterisk es una completa central PBX basado en software, bajo el sistema operativo Linux Centos que permite construir aplicaciones de comunicaciones tan complejas o avanzadas como se desee sin incurrir en altos costos y con más flexibilidad que cualquier sistema de telefonía.

Linux Centos es la distribución de linux que sirve como Sistema Operacional, está basado en Linux Red Hat Enterprise.



Asterisk es el núcleo de telefonía y cuando hablamos de Asterisk incluimos también los drivers de Zapata Telephony (zaptel) y la librería para soporte RDSI.

Este laboratorio empieza desde la instalación del servidor Asterisk. Luego de la instalación se procede a asignarle una dirección IP dentro de la red de la facultad procurando no crear conflicto con una dirección que ya se encuentre ocupada.

La administración de la central Asterisk se realiza vía web, introduciendo la dirección IP asignada en la máquina virtual en el explorador. Se crean extensiones SIP que luego se validan en los softphones para establecer una llamada.

Asimismo se instalan los módulos que se pueden agregar en el Asterisk.

V. Conocimientos previos

- Máquina Virtual
- Asterisk
- Comandos de Asterisk
- Servicios que brinda Asterisk.
- Laboratorio 5: Introducción a Hipath 2000

VI. Procedimiento

Actividad 1: Instalación del sistema operativo Linux

1. Inserte el cd de Trixbox y haga click en crear una nueva máquina virtual.
2. Inmediatamente va a detectar el Trixbox en Disco Instalador y de click en siguiente.
3. Seleccione el sistema operativo y la versión correspondiente, la cual es Linux y CentOS respectivamente. Pide el espacio máximo del disco duro.
4. Seleccione la opción de encender la máquina virtual inmediatamente después de la instalación en "Power on this virtual machine".
5. Inmediatamente después de la instalación cargará el trixbox
6. Seleccione el teclado, en este caso Estados Unidos.
7. Elija la zona horaria
8. Presione ok.
9. Se le pedirá una contraseña, luego de confirmar su contraseña iniciará el formato de su disco duro y la instalación de los paquetes. El tiempo de esta dependerá de la capacidad del PC.



10. Una vez que se termina la instalación se le pedirá el nombre de usuario el cual es root y un password, que viene a ser el que se definió anteriormente. Tal como se muestra en la figura 2.

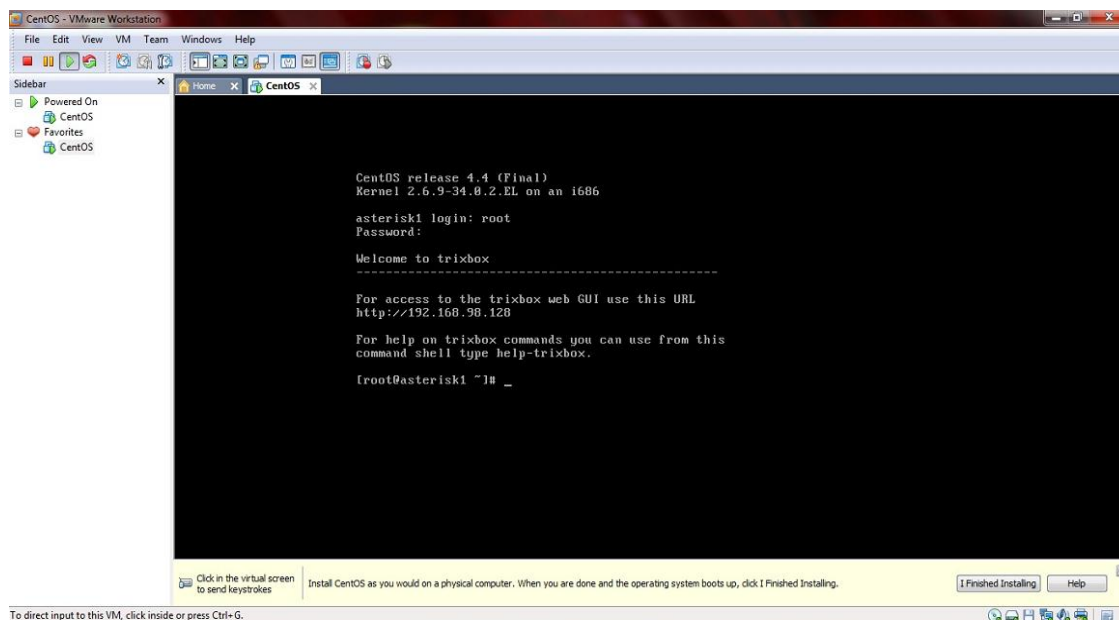


Fig. 1 Asterisk login

11. Cuando la instalación termine apague la máquina virtual con el comando “shutdown -h now”.

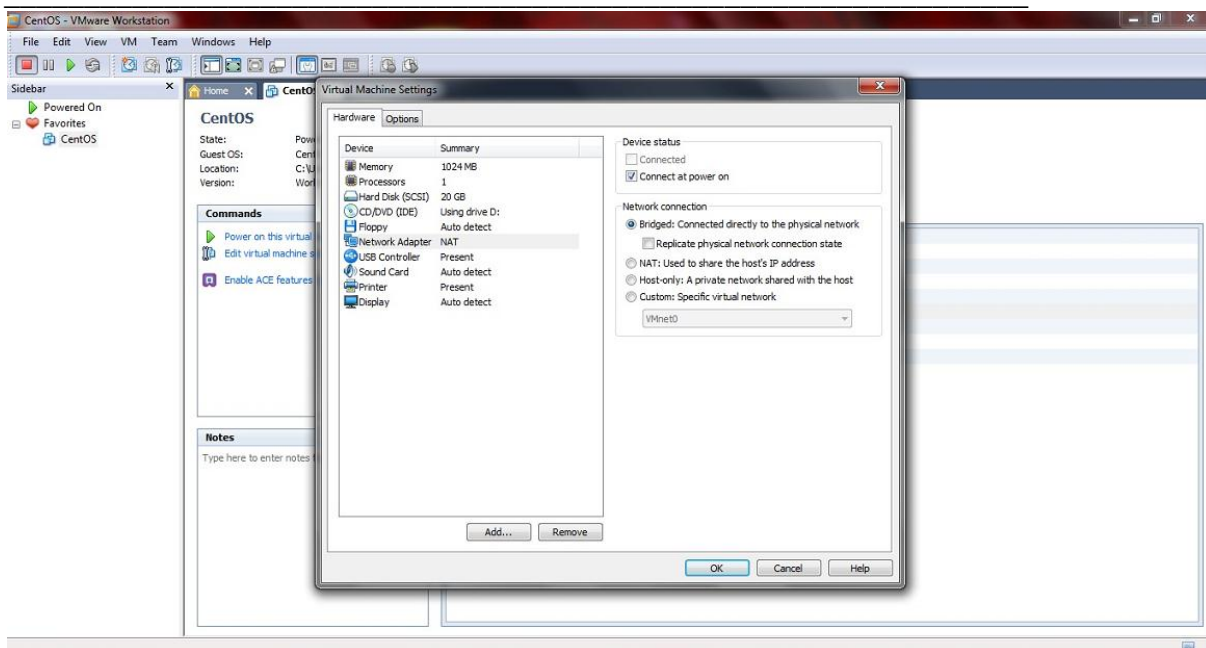


Fig. 2 Instalación de máquina virtual

12. Luego se debe cambiar en el sistema operativo CentOS pestaña de dispositivos, opción adaptador de red la conexión de red NAT por Bridged tal como se muestra en la figura 1.

Actividad 2: Configuración de la dirección IP del Asterisk

1. Cuando cargue el sistema operativo Linux Centos aparecerá el login para ingresar al asterisk y luego el password. El login es root mientras que la contraseña es definida por el usuario. En este caso la contraseña es electrónica.
2. Para salir de Asterisk presione Control + Alt
3. Inicialice la aplicación Advanced Port Scanner para detectar todas las direcciones IP que se encuentran ocupadas dentro de la red de la UNI.
4. Elija una dirección que no se encuentra ocupada dentro del rango 192.168.73.1 hasta 192.168.73.255. En este caso elegimos 192.168.73.3.

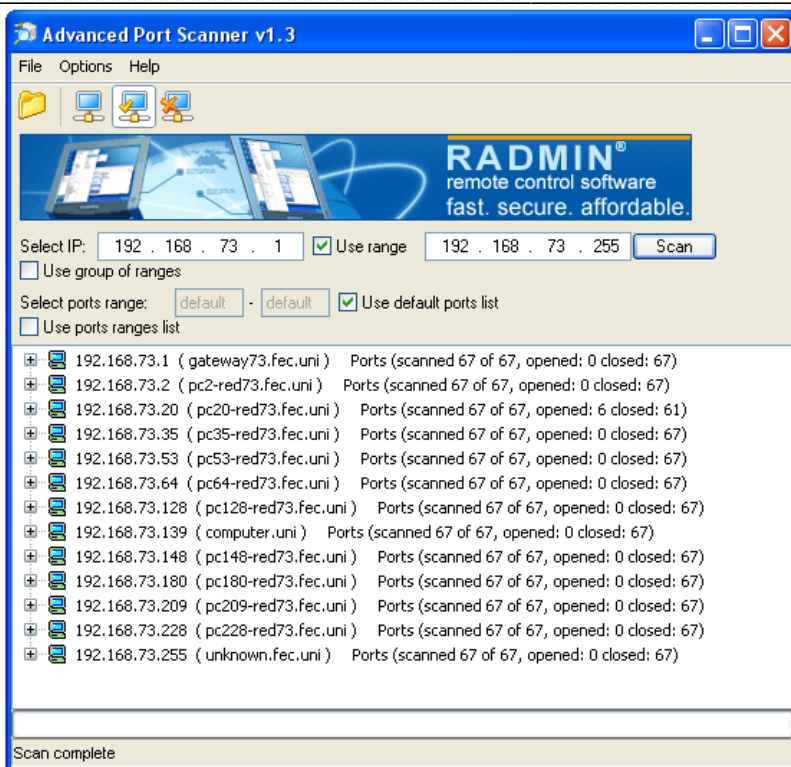


Fig. 3 Advanced Port Scanner v1.3

5. Introduzca el comando netconfig para cambiar la dirección IP que contiene por defecto el Asterisk y presione yes.

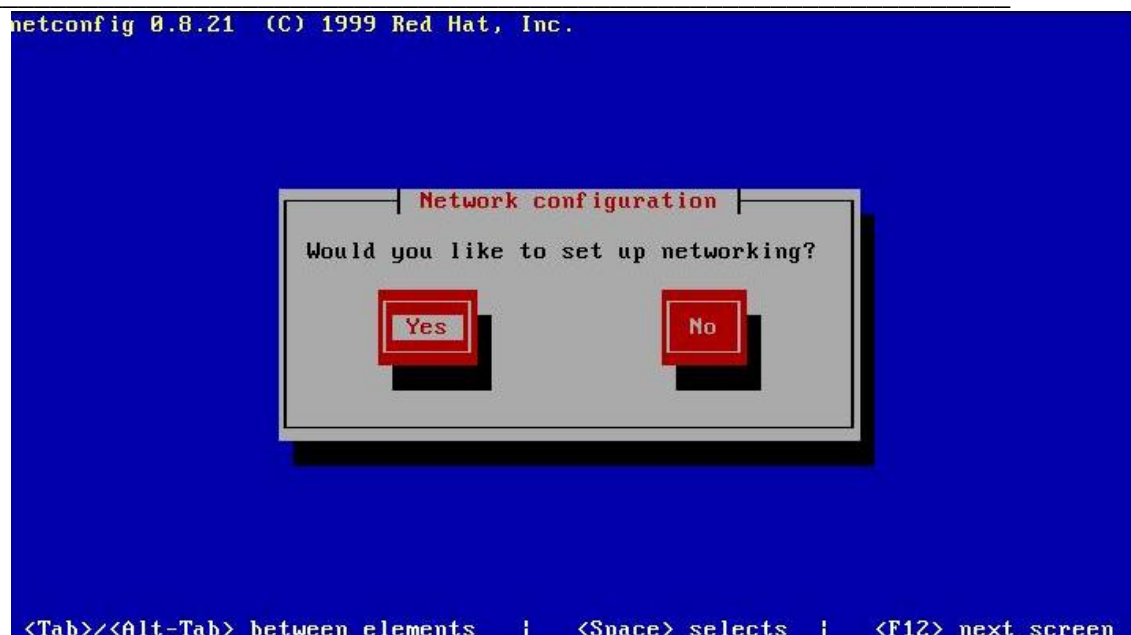


Fig. 4 Comando netconfig

6. Ingrese los parámetros de configuración IP.
7. Establezca la dirección IP en 192.168.73.3; máscara 255.255.255.0 y tanto el Gateway por defecto como el primary name server en 192.168.1.1.
8. Presione ok.

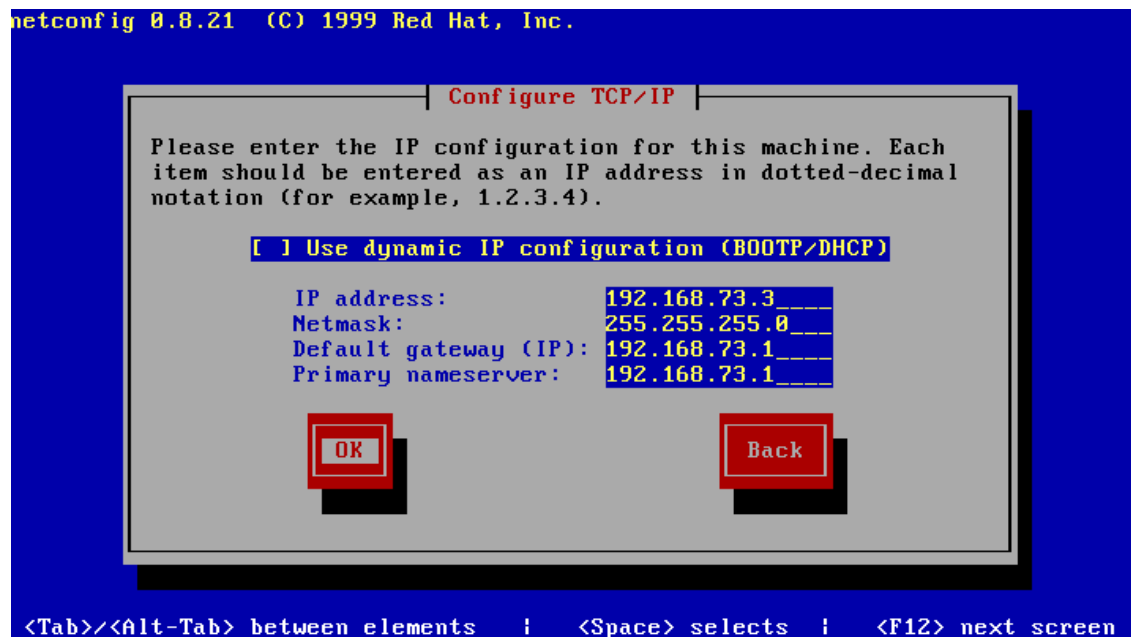


Fig. 5 Configuración TCP/IP



9. Luego escriba el comando `service network restart` para reiniciar el servicio de red.
10. Ingrese el comando `ifconfig` para verificar si la información de los parámetros IP está configurada correctamente.

```
[root@asterisk1 ~]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0C:29:F4:76:E6
          inet addr:192.168.73.2  Bcast:192.168.73.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fef4:76e6/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1149 errors:0 dropped:0 overruns:0 frame:0
          TX packets:122 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:76150 (74.3 KiB)  TX bytes:8106 (7.9 KiB)
          Interrupt:5 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:162 errors:0 dropped:0 overruns:0 frame:0
          TX packets:162 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:25839 (25.2 KiB)  TX bytes:25839 (25.2 KiB)

[root@asterisk1 ~]#
```

Fig. 6 Comando `ifconfig`

Actividad 3: Añadir extensiones en el Asterisk vía web

1. Abra una ventana de su explorador.
2. Escriba la dirección del trixbox definida en el Linux Centos <http://192.168.73.3>.
3. En la parte superior derecha busque Modo de usuario y haga click en el vínculo interruptor para poder entrar al Asterisk.

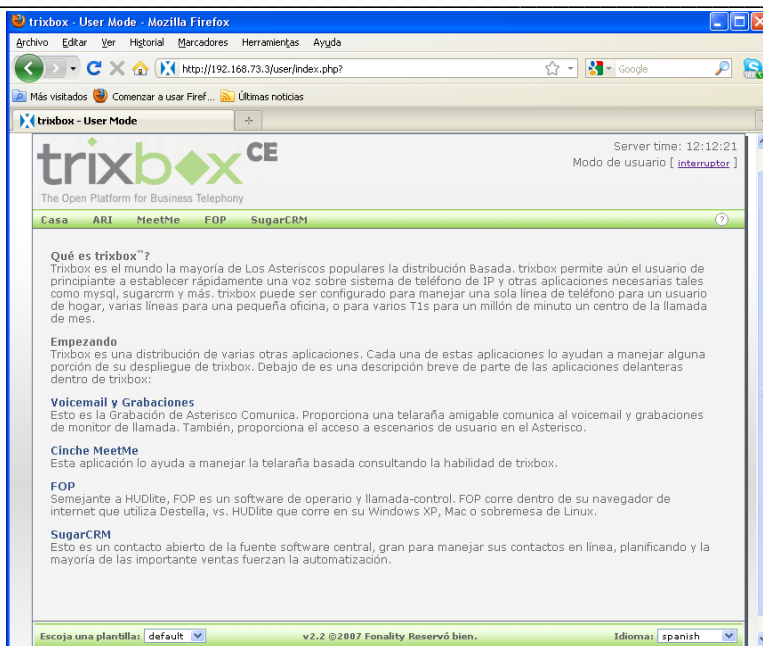


Fig. 7 Página principal de Trixbox

4. A continuación le pedirá un nombre de usuario y un password. El nombre de usuario es maint, el password es "password".
5. Seleccione Asterisco de la barra de menú y haga click en Free PBX para ingresar a las configuraciones.

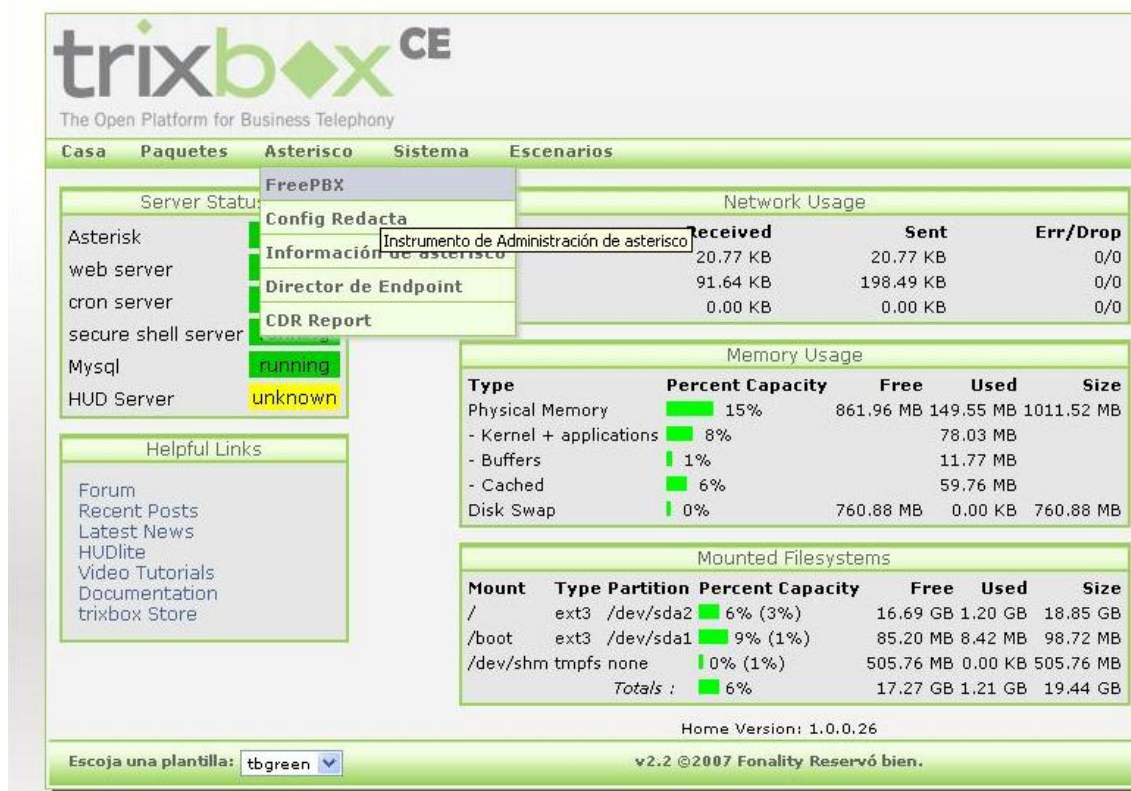


Fig. 8 Instrumento de Administración de Asterisk

- En la parte superior derecha cambie el idioma a español.
- Seleccione Configuración de la barra de menú y se le desplegará un pequeño menú a la izquierda.
- En dicho menú elija configuraciones generales y configure todos los parámetros tal y como se muestra en la figura 9.
- Cuando haya terminado con todas las configuraciones que se muestran en la figura 9 de click en enviar cambios.
- De click en Apply Configuration Changes.



The screenshot displays the freePBX 2.2.1 web interface. The top navigation bar includes links for 'Configuración', 'Herramientas', 'Informes', 'Panel', and 'Grabaciones'. The 'freePBX' logo is in the top right corner. A sidebar on the left lists configuration categories: 'Básico', 'Gestión de usuarios', 'Extensiones', 'Configuraciones Generales' (highlighted), 'Rutas Salientes', 'Troncales', 'Inbound Call Control', and 'Rutas Entrantes'. The main content area is titled 'Configuración' and contains several sections: 'Opciones de marcado' with fields for 'Opciones de Marcado' and 'Asterisk Outbound Dial command options'; 'Buzón de Voz' with settings for voicemail duration, prefix, and message type; 'Directorio de la empresa' with a search dropdown and a checkbox for playing extension numbers; 'Maquina de FAX' with fields for fax machine extension and email addresses; 'International Settings' with a country dropdown and 24-hour format selector; and 'Security Settings' with a checkbox for anonymous inbound SIP calls. An 'Enviar cambios' button is at the bottom. A decorative graphic of colored squares is in the bottom right corner.

Fig. 9 Configuraciones generales

11. En el menú de Configuración elija extensiones para añadir una extensión.

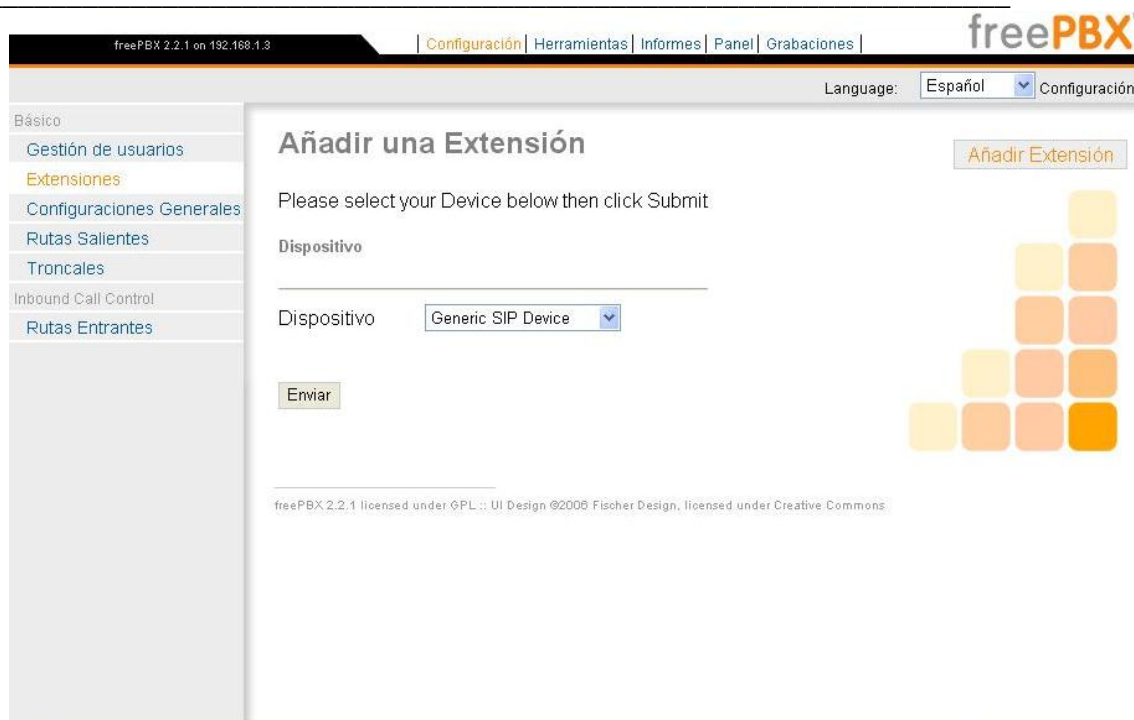


Fig. 10 Añadir extensión

12. Despliegue la pestaña de dispositivo y seleccione Generic SIP Device que es el protocolo que utilizan los softphones. Click en enviar.

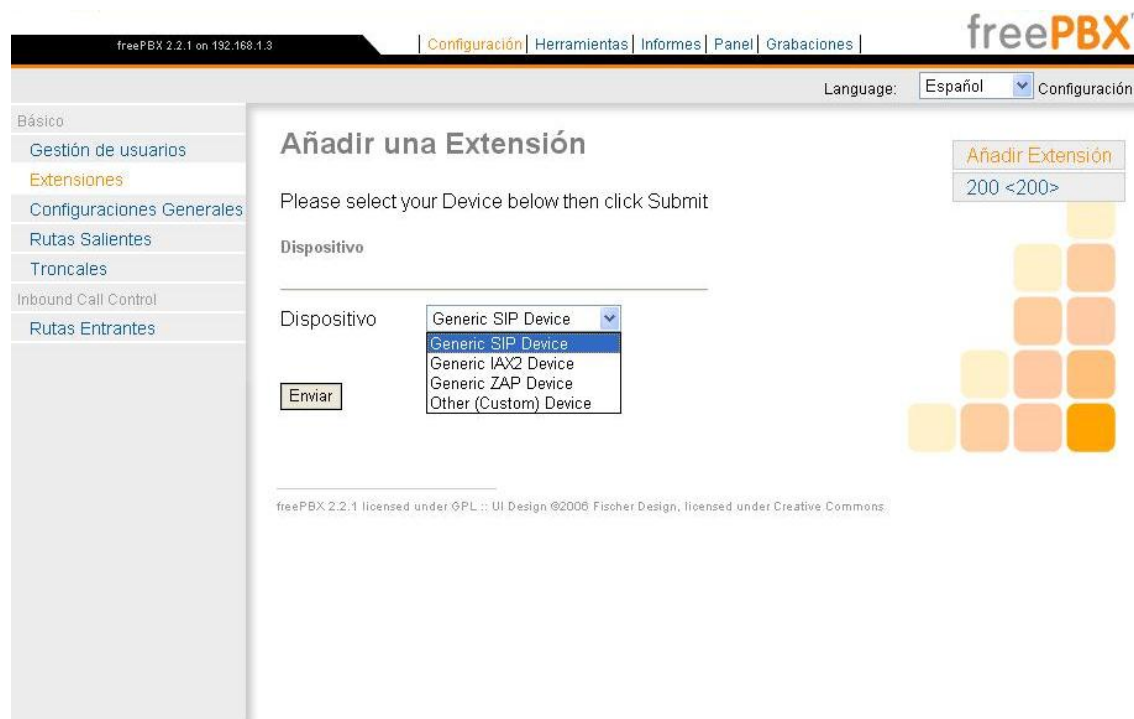


Fig. 11 Protocolo de extensión

13. Ingrese el número de extensión, nombre de asociado y el secret. Tanto el número de extensión como el secret deben estar en 200. El nombre de asociado puede ser el de su preferencia pero por comodidad también establézcalo en 200.



Fig. 12 Parámetros de las extensiones

14. Para guardar los cambios de click en enviar.
15. De click en Apply Configuration Changes.
16. Agregue 4 extensiones más siguiendo el mismo procedimiento antes descrito.

Actividad 4: Comunicación entre softphones

1. Realice el mismo procedimiento efectuado en la actividad 4 del laboratorio 5 correspondiente a la Hipath 2000.

Actividad 5: Limpieza

1. Apague la máquina virtual con el comando "shutdown -h now".
2. Desinstale Asterisk y el Sistema Operativo Centos.

VII. Preguntas de control

1. ¿Qué función posee el protocolo IAX2 y ZAP en Asterisk?
2. ¿Cómo se establece una conferencia en Asterisk?
3. ¿Para qué se utiliza el PIN de administrador en una conferencia?



Laboratorio No. 4: Configuración de Servicios en PBX virtual

Modulo	Redes de Telefonía		
Tipo Práctica	<input type="checkbox"/> Laboratorio <input type="checkbox"/> Simulación		
Unidad Temática			
No Alumnos por práctica	2	Fecha	
Nombre del Profesor			
Nombre(s) de Alumno(s)			
Tiempo estimado		Vo. Bo. Del Profesor	
Comentarios			

Objetivos de la práctica de laboratorio

I. Objetivo general

1. Configurar los servicios que brinda la PBX virtual Asterisk.

II. Objetivos específicos

1. Instalar el servidor Asterisk a través de una máquina virtual.
2. Añadir extensiones SIP.
3. Establecer la comunicación entre softphones.

III. Medios a utilizar

- Equipo de cómputo
- Router o Switch
- Disco de instalación de Trixbox
- Softphone Zoiper o Xlite

IV. Introducción

Asterisk es una completa central PBX basado en software, bajo el sistema operativo Linux Centos que permite construir aplicaciones de comunicaciones tan complejas o avanzadas como se desee sin incurrir en altos costos y con más flexibilidad que cualquier sistema de telefonía.



Asterisk ofrece las funciones estándar conocidas de todas las centralitas tipo Cisco, Avaya, Alcatel o Siemens como desvíos, capturas y transferencias de llamada o multiconferencias. Sin embargo, permite ampliar esta paleta con funciones avanzadas e inteligentes como buzón de voz, IVT, CTI, ACD y otras medidas encaminadas a minimizar tiempos y maximizar la efectividad de las llamadas.

Concretamente, Asterisk ofrece entre muchas otras, estas funciones:

- Conexión con líneas de telefonía tradicional, mediante interfaces tipo analógico (FXO) para líneas de teléfono fijo o bien móvil y RDSI (BRI o PRI).
- Soporte de extensiones analógicas, bien para terminales telefónicos analógicos, terminales DECT o bien equipos de fax.
- Soporte de líneas (trunks) IP: SIP, H323 o IAX.
- Soporte de extensiones IP: SIP, SCCP, MGCP, H323 o IAX.
- Música en Espera basada en archivos MP3 o similar.
- Funciones básicas de usuario
- Transferencias (directa o consultiva)
- Capturas (de grupo o de extensión)
- Conferencia múltiple
- Aparcamiento de llamadas (Call parking)
- Llamada directa a extensión
- Retrollamada - Callback (llamada automática cuando disponible).
- Paging - Megafonía a través del altavoz del teléfono.
- DND

V. Conocimientos previos

- Máquina Virtual
- Asterisk



- Comandos de Asterisk
- Servicios que brinda Asterisk.

VI. Procedimiento

Actividad 1: Instalación de la PBX virtual

Instale la PBX virtual siguiendo el procedimiento explicado en el laboratorio número 4.

Actividad 2: Instalación de módulos

1. Ingrese al menú Herramientas y escoja a la izquierda la opción “Gestor de Módulos”.
2. Active todos los módulos que no se encuentran instalados marcando la primera columna de las tablas que aparecen para agregar. Seleccione Acción y luego instalar.
3. Una vez que todos los módulos están listos para instalarse elija procesar.
4. Haga click en Confirmar y luego en Apply Configuration Changes para guardar los cambios.

Module Administration

[Check for updates online](#)

Reset Process

Module Type Version

Basic

Core	setup	1.2	Enabled
Feature Code Admin	setup	1.0.4	Enabled
Voicemail	setup	Not Installed (Locally available)	
Action	<input type="radio"/> No Action		
Description	<input checked="" type="radio"/> Install		
Changelog			

Fig. 13 Gestor de módulos



Actividad 3: Programación de servicios

Actividad 3.1: Conferencia

1. Seleccione Conferencias dentro del menú de Configuraciones. A continuación aparecen 4 parámetros principales para modificar: El número de conferencia, nombre de conferencia, el PIN de usuario y el PIN de administrador
2. El número de conferencia corresponde a un número virtual al cual todas las extensiones pueden llamar para establecer la conferencia. Al ingresar a la conferencia el primer participante escuchará un mensaje indicando que “es el único en esta conferencia” y a partir del segundo participante podrán conversar entre sí.
3. Elija un número de conferencia de tal forma que no cree conflicto con los números de extensiones. En este caso 150, tal como aparece en la figura 23.
4. Escriba un nombre para la conferencia.
5. Los campos correspondientes a PIN de usuario y de administrador son con el objetivo de ingresar una contraseña de entrada para realizar la conferencia.
6. Cambia la opción de música en espera a YES mientras se establece la conferencia.
7. De click en enviar cambios y luego en Apply Configuration Changes.



Add Conference

[Add Conference](#)

Add Conference

conference number:
conference name:
user PIN:
admin PIN:

Conference Options

join message:
leader wait:
quiet mode:
user count:
user join/leave:
music on hold:
allow menu:



Fig. 14 Agregar conferencia

Actividad 3.2: Música en espera

1. Seleccione Música en espera dentro del menú de Configuraciones.
2. Agregue un archivo mp3 de su preferencia en la pestaña Examinar.
3. Luego seleccione Upload y a continuación Apply Configuration Changes para guardar los cambios.

Actividad 3.3: Administrador de conferencia

1. Ingrese a la conferencia con un softphone, marcando el número destinado para este servicio en la actividad 6.1.
2. Cuando se realice la llamada a la conferencia aparecerá la música en espera elegida en la actividad 6.2, mientras entra otra extensión a dicha conferencia.



3. Abra la página principal de Trixbox con dirección 192.168.73.3 y haga click en el vínculo que dice “MeetMe”.
4. Coloque el número de la sala de conferencia que destinó en la actividad 6.1 y haga click en “connect”. Aquí se observarán las extensiones que se encuentran dentro de la sala.
5. Agregue una extensión más en la sala de conferencias, llamando al número de conferencia desde otro softphone.
6. Inmediatamente se establece la conferencia.
7. Observe los parámetros que se reflejan mientras anexa otra extensión a la lista de conferencias.
8. Seleccione MUTE en una de las extensiones y describa lo que pasa.
9. Seleccione KICK en una de las extensiones y describa lo que pasa.

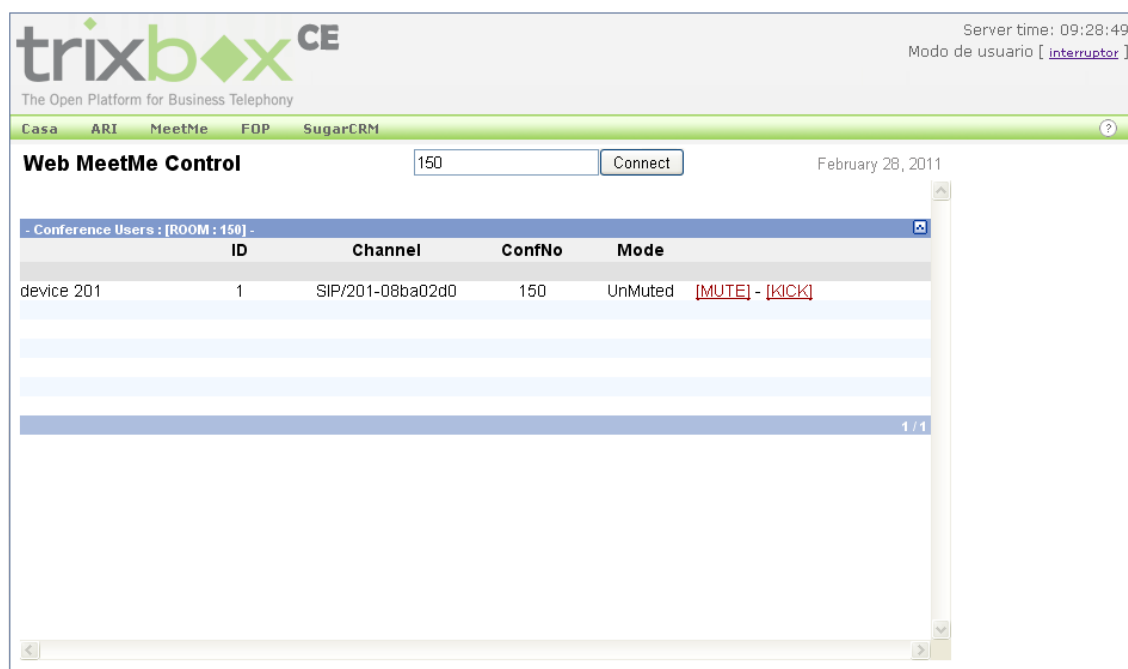


Fig. 15 Web MeetMe Control



Actividad 4: Conferencia

1. Marque la extensión con la cual se desea comunicar.
2. Cuando la extensión a la que se llame levante, aparecerán varias opciones en el display. Seleccione Iniciar conferencia.
3. A continuación se pedirá el otro número con el cual se desea establecer la conferencia. Digite dicho número.
4. Una vez que contesta la otra extensión a la que se llamó, aparecerá en el display Conferencia? A continuación pulse confirmar. De esta manera ya se tiene entablada la conferencia.

VII. Preguntas de control

4. ¿Para qué sirve la música en espera?
5. ¿Qué beneficios trae las conferencias?
6. ¿Qué es web meetme control?



Laboratorio No. 5: Introducción al módulo EE-PM *

Modulo	Redes de Telefonía		
Tipo Práctica	<input type="checkbox"/> Laboratorio <input type="checkbox"/> Simulación		
Unidad Temática			
No Alumnos por práctica	2	Fecha	
Nombre del Profesor			
Nombre(s) de Alumno(s)			
Tiempo estimado		Vo. Bo. Del Profesor	
Comentarios			

Objetivos de la práctica de laboratorio**I. Objetivo general**

1. Examinar la funcionalidad básica del sistema PCM/EV.

II. Objetivos específicos

1. Observar las señales que se producen en el simulador de línea a través del osciloscopio.
2. Verificar las conexiones de los teléfonos, observando las pulsaciones del LED correspondiente a ocupado.

III. Medios a utilizar

- Unidad PCM/EV
- Teléfonos del equipo
- Osciloscopio
- Memoria USB

IV. Introducción

El módulo PCM/EV es un módulo perteneciente a la serie Telefonía Fija cuyo propósito es el desarrollo de cursos teóricos experimentales relacionados con el



estudio de todos los conceptos, equipos y sistemas utilizados en la telefonía moderna.

Es un sistema utilizado para investigar los aspectos principales relacionados con la codificación, conmutación y transmisión digital de señales PCM y desarrolla las funciones típicas de una central telefónica y un multiplex.

Las especificaciones relativas a las secciones que constituyen el sistema PCM/EV se ajustan a los estándares del comité europeo de normalización European Conference of Postal and Telecommunications Administrations (CEPT).

Como nodo de conmutación digital, el sistema PCM/EV incluye tres niveles de procesamiento de las señales de telefonía:

- La codificación y la decodificación PCM de las fonías relacionadas con los terminales de usuario.
- La formación y la gestión de las multiplexaciones PCM en el interior de la central, que son utilizadas por la matriz de conmutación para establecer los circuitos de fonía.
- La conversión entre las multiplexaciones PCM internas y el sistema primario de la línea saliente que, en las redes, se conecta con otro nodo de conmutación o con una prolongación de central.

El sistema PCM/EV está constituido por los siguientes componentes:

- Interfaz con las líneas de usuario.
- Unidad de conmutación digital.
- Interfaz con la línea externa.
- Línea simulada.



-
- Receptor de línea.
 - Transmisor de línea.
 - Base de tiempos
 - Generador de tonos.

El propósito de esta práctica es la observación y el análisis de como las comunicaciones se ven afectadas por factores como el ruido y la atenuación y la forma en que estos elementos son destructivos a la hora de entablar una comunicación.

Mediante la observación de señales en el simulador de línea cuando se realizan llamadas el estudiante puede establecer una comparación entre estas señales cuando no son afectadas por el ruido y la atenuación y estas mismas señales pero introduciéndoles los componentes ruido y atenuación.

En este laboratorio también se hace la verificación de las conexiones entre los usuarios y le enseña al estudiante cómo funciona la central cuando se realizan llamadas dentro del sistema es decir internas y cuando se hacen llamadas fuera del sistema o externas.

V. Conocimientos previos

- PCM (Modulación por impulsos codificados).
- Marcación por pulso o Decadico.
- Marcación por tonos o DTMF.
- Establecimiento de una llamada.

VI. Procedimiento

El escenario a implantarse se muestra en la figura 1. Aquí se presentan los medios a utilizar como son el equipo PCM/EV y los teléfonos:

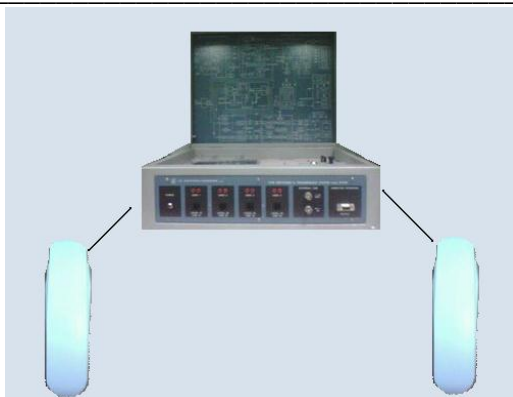


Fig. 1 Escenario del laboratorio

Actividad 1: Ajuste de parámetros

1. Conecte el módulo PCM/EV al suministro eléctrico y oprima el switch de encendido/apagado.
2. Conecte los 4 teléfonos a los bornes de línea del panel del modulo.
3. Verifique que todos los LED de visualización de las alimentaciones y el LED Test Mode estén encendidos.
4. Verifique que los teléfonos están en modo Decadico (pulso), si no es así cámbielo a dicho modo.
5. Seleccionar el potenciómetro Noise al mínimo.
6. Seleccionar el potenciómetro Attenuation al mínimo.
7. Ponga el selector Remote Mode en la posición Master.
8. Ponga el selector Control Selection en la posición Local.
9. En el panel que se localiza al lado derecho se encuentra un led que se llama Sync Loss, observe este led con los parámetros que se pidieron al inicio de la actividad.
10. Siga observando el led Sync Loss y empiece a variar los parámetros Noise y Attenuation.
11. Anote lo que ocurre.



Actividad 2: Prueba con osciloscopio

1. Conecte dos sondas de pruebas al osciloscopio.
2. Conecte una de las sondas del osciloscopio a TP30 y a tierra y la otra sonda a TP32 y tierra asegurándose primero que los parámetros Noise y Attenuation se encuentren en cero.
3. Ajuste las escalas del osciloscopio 200mV/Div y 500nsegT/Div para observar con mayor claridad las señales.
4. Para visualizar con mayor claridad la imagen haga una captura de pantalla con el botón RUN/STOP del osciloscopio y luego varíe el T/Div.
5. Guarde la señal capturada en su memoria USB y anote los datos más relevantes que observe en dicha señal.
6. Presione nuevamente el botón RUN/STOP para continuar con la visualización normal de la señal.
7. Una vez que observe las señales en TP30 y TP32 con los parámetros Noise y Attenuation en cero, mueva los potenciómetros pertenecientes a estos parámetros y observe como la señal de TP32 varia conforme aumenta un potenciómetro primero y el otro después.
8. Invierta el orden en que manipula los parámetros.
9. Guarde la señal de TP32 en su memoria USB y anote los resultados obtenidos.
10. Conecte una de las sondas de prueba del osciloscopio a TP33 y a tierra y la otra sonda a TP34 y a tierra. Asegúrese que los parámetros Noise y Attenuation se encuentren en cero.
11. Ajuste las escalas del osciloscopio V/Div a 100mV y T/Div a 500nSeg. para observar con mayor claridad las señales.
12. Haga una captura de pantalla.



-
13. Guarde la señal capturada en su memoria USB y anote los datos más relevantes de ambas señales.
 14. Ahora mueva los potenciómetros pertenecientes a los parámetros mencionados anteriormente y observe como la señal varía conforme aumenta un potenciómetro primero y el otro después. Luego invierta el orden en que manipula los parámetros.
 15. Guarde la señal capturada en su memoria USB y anote los datos más relevantes que observados.

Actividad 3: Verificación de conexiones

1. Levante el teléfono #1 (User 1). Escuche el tono de invitación a marcar.
2. Verifique en el panel Display que se encienda el LED correspondiente a Switch Hook Detector del user 1.
3. Llame a alguno de los teléfonos restantes que se encuentran conectados en el modulo y perciba que al marcar la primera cifra en el teléfono el tono de invitación a marcar no se escucha mas.
4. Para llamar a números que son de conexión interna marque: 01 para el teléfono User 1, 02 para el teléfono User 2, 03 para el teléfono User 3 y 04 para el teléfono User 4 y para los de conexión externa marque: 51 para el teléfono User 1, 52 para el teléfono User 2, 53 para el teléfono del User 3 y 54 para el teléfono User 4.
5. Verifique que se pueden efectuar solamente las conexiones internas (selección 0X) y no las externas (selección 5X), para esto descuelgue el teléfono #1 y llame a los teléfonos restantes de la selección 0X. Espere la señal de llamada al teléfono. seleccionado escuchando el tono de línea audible en el teléfono #1(User 1).
6. Levante el teléfono al que se está llamando y verifique que se establece la llamada.



-
7. Termine la llamada
 8. Luego levante el teléfono #1 (User 1) y llame a alguno de los teléfonos de conexión externa es decir 5X. Una vez marcado el teléfono de su elección observe las pulsaciones del LED correspondiente a ocupado en panel Display.
 9. Termine la llamada.
 10. Repita toda la actividad 3 con los teléfonos programados en modo DTMF. En este se podrá escuchar en línea los tonos al marcar cada tecla y su vez se podrá observar que los leds del sinóptico a la salida del decodificador DTMF visualizan el código binario correspondiente a la cifra marcada.

VII. Preguntas de control

2. ¿Qué es PCM?
3. ¿Por qué se llama sistema PCM/EV?
4. Explique cómo se ven afectadas todas las señales observadas en la actividad 2 cuando se aumentan los parámetros Noise y Attenuation.
5. En la actividad 2 ¿cuál es la diferencia entre la señal que se observa en TP33 y la señal en TP34 cuando los parámetros Noise y Attenuation están establecidos en cero? ¿Qué pasa con estas señales cuando los parámetros Noise y Attenuation son aumentados? ¿la diferencia entre ambas señales se mantienen?
6. ¿Cuál es la diferencia cuando se llama en modo decádico a cuando se llama en modo DTMF?
7. Entre los parámetros Noise y Attenuation ¿cuál es el parámetro que más afectaba las señales observadas en los distintos puntos de prueba?
8. Considera usted que los parámetros Noise y Attenuation afectan las comunicaciones alámbricas de igual manera en que se vieron afectadas las señales en el modulo PCM/EV? Fundamente su respuesta.



-
9. ¿Qué hacen las compañías telefónicas para que se dé la concreción de las comunicaciones entre abonados con un nivel de claridad y comodidad aceptable?



Laboratorio No. 6: Codificación HDB3

Modulo	Redes de Telefonía		
Tipo Práctica	<input type="checkbox"/> Laboratorio <input type="checkbox"/> Simulación		
Unidad Temática			
No Alumnos por práctica	2	Fecha	
Nombre del Profesor			
Nombre(s) de Alumno(s)			
Tiempo estimado		Vo. Bo. Del Profesor	
Comentarios			

Objetivos de la práctica de laboratorio

I. Objetivo general

1. Observar el código de línea transmitido en una llamada telefónica.

II. Objetivos específicos

1. Visualizar como los componentes de polaridad de la señal HDB3 separado en líneas distintas.
2. Comprender como se atenúa una señal en una línea.

III. Medios a utilizar

- Unidad EE-PM con teléfonos
- Osciloscopio

IV. Introducción

La finalidad de este ejercicio es la de poner en evidencia el proceso de codificación HDB3 en la señalización saliente. El interfaz suministra al transmisor de línea las dos componentes de polaridad de la señal HDB3, separadas en líneas distintas TXA y TXB, con la misma polaridad positiva. En la salida del transmisor está presente la señal HDB3 compuesta. Para analizar la codificación HDB3 en los datos de sincronismo, la señalización y canales de voz que constituyen las tramas del sistema primario, habrá que tener presente que: en el intervalo temporal 0 se alternan configuraciones de alineación (tramas pares) con configuraciones de no alineación (tramas

Impares); en el intervalo temporal 16 los datos de señalización son fijos, en el caso del sistema didáctico analizado, salvo su sustitución con la alineación de multitrama una vez cada 16 tramas; los datos de voz son variables por naturaleza y es suficiente el cambio de un solo bit en los canales de voz para cambiar la configuración de todos los impulsos sucesivos. El caso más favorable se refiere a los canales de transmisión utilizados que son recibidos como secuencias bits todos iguales a "1"; por ello, es más fácil observar la ley alternancia incluida en la codificación HDB3. Por ejemplo, para los canales 17-31 y en situación de secuencias predominantes de las componentes TXA y TXB, así la configuración de la señal HDB3 son las que se muestran en la Figura 1. Observar en el osciloscopio las secuencias de la figura con las fases en parte superpuestas, pero con un caso predominante sobre los demás.

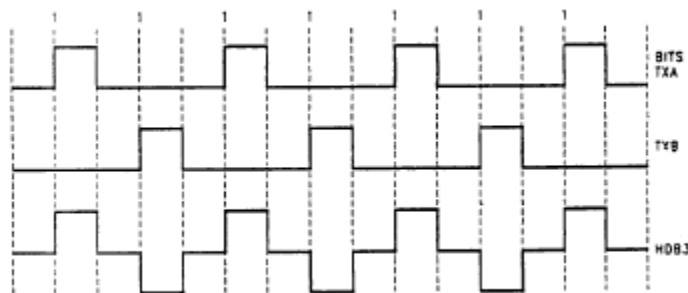


Figura 1 Código HDB3

V. Procedimiento

El escenario a implantarse se muestra en la Figura 2. Aquí se presentan los medios a utilizar como son el equipo PCM/EEPM, los teléfonos y el osciloscopio:

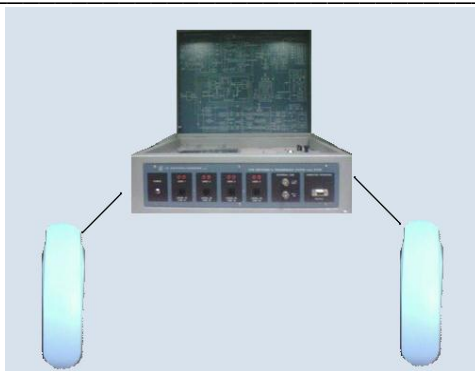


Figura 2 Escenario a usar

Actividad 1: Códigos de líneas HDB3 en telefonía.

1. Ajuste el módulo PCM-EEPM en MODO TEST, para ello diríjase al panel de control de selección y ubique el switch en modo local y luego presione el push botón (MODO SELECT) para cambiar a MODE TEST. Confirme dicho modo con el led rojo q se encenderá en panel.
2. Conecte dos sondas de pruebas al osciloscopio.
3. Conecte una de las sondas del osciloscopio a TP27 y a tierra y la otra sonda a TP28 y tierra asegurándose primero que los parámetros Noise y Attenuation del módulo PCM se encuentren en cero.
4. Observe las señales mostradas y ajuste las escalas del osciloscopio 200mV/Div y 500nsegT/Div para observar con mayor claridad las señales.
5. Para visualizar con mayor claridad la imagen haga una captura de pantalla con el botón RUN/STOP del osciloscopio y luego varié el T/Div.
6. Guarde la señal capturada en su memoria USB y anote los datos más relevantes que observe en dicha señal.
7. Presione nuevamente el botón RUN/STOP para continuar con la visualización normal de la señal.



8. Varié las ranuras de tiempo pulsando sobre los puch botón desde 0 hasta 31, haga énfasis en las ranuras 1,2,3,4 observe y anote los resultados visualizados del comportamiento de la señal.
9. Una vez que observo las señales en TP27 y TP28 con los parámetros Noise y Attenuation en cero, desplace de manera intermitente la sonda de TP27 en TP30.
10. Haga una captura de pantalla con el botón RUN/STOP del osciloscopio y luego varié el T/Div.
11. Guarde la señal capturada en su memoria USB y anote los datos más relevantes que observo en dicha señal.
12. Presione nuevamente el botón RUN/STOP para continuar con la visualización normal de la señal.
13. Desplace la sonda de prueba alternativamente la sonda ubicada en TP28 en TP30.
14. Capture la imagen y guarde la señal capturada en su memoria USB, anote los datos más relevantes que observo en dicha señal.
15. Presione nuevamente el botón RUN/STOP para continuar con la visualización normal de la señal.
16. Varié los potenciómetros de RUIDO y ATENUACION, observe y anote los resultados.

Actividad 2: Códigos de líneas HDB3 durante una llamada.

1. Levante el teléfono número 2 y marque al teléfono 3.
2. Realice todo el procedimiento realizado en la actividad 1, manteniendo la llamada entre los teléfonos 2 y 3, y haciendo énfasis en las ranuras de Tiempo 2 y 3.
3. Anote las diferencias encontradas.



VI. Preguntas de control

1. ¿Qué es HDB3?
2. ¿Qué sucede cuando en la transmisión de datos existen más de 4 ceros consecutivos?
3. ¿Qué sucede con la señal HDB3 cuando se varían los potenciómetros de Atenuación y Ruido.
4. ¿Qué sucede con los componentes TXA y TXB cuando se observa TP30?



Laboratorio No. 7: Recepción de la señal HDB3

Curso	Capacitación en telefonía IP		
Modulo	Redes de Telefonía	Grupo	
Tipo Practica	<input type="checkbox"/> Laboratorio <input type="checkbox"/> Simulación		
Unidad Temática			
No Alumnos por practica	1	Fecha	
Nombre del Profesor			
Nombre(s) del Alumno(s)			
Tiempo estimado	45 minutos	Vo. Bo. Del Docente	
Comentarios			

Objetivos de la práctica de laboratorio

I. Objetivo General

1. Observar las ranuras de tiempo (Time Slot o Trama) PCM de transmisión y recepción que forman los circuitos de telefonía.

II. Objetivos específicos

1. Identificar en que trama o ranura de tiempo se está transmitiendo los datos de una llamada.
2. Observar el comportamiento de los datos transmitidos durante una llamada telefónica.
3. Mostrar cómo se transmiten las tramas en canales distintos.

III. Medios a utilizar

- Unidad EE-PM
- 4 Teléfonos del Equipo
- Osciloscopio

IV. Introducción

En este laboratorio se analiza el proceso de recepción de la señal HDB3.



La señal que llega a la entrada del receptor es el resultado de las características del transmisor y de la línea.

Antes de llegar al receptor la señal es ecualizada por un circuito (FILTER) que compensa la respuesta en frecuencia de la línea.

En el receptor un circuito de retroacción compensa en modo adaptativo los efectos debido a líneas de longitud y de características diferentes.

Las fases restantes de la recepción (extracción de la señal de reloj, muestreo de la señal HDB3, detección de las componentes RxA y RxB correspondientes a las 2 polaridades del HDB3).

V. Conocimientos previos

- Codificación de Línea
- Codificación HDB3

VI. Procedimiento

El escenario a implantarse se muestra en la Figura 3. Aquí se presentan los medios a utilizar como son el equipo PCM/EEPM, los teléfonos y el osciloscopio:

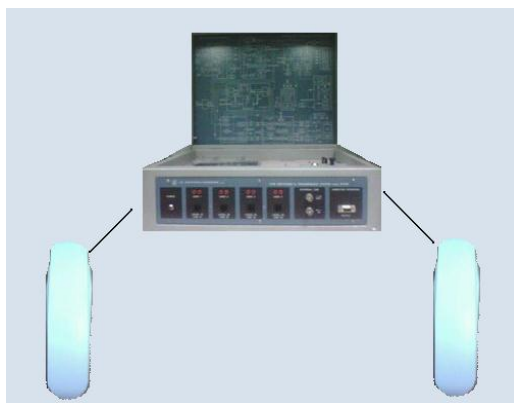


Figura 3 Escenario a implementar

Actividad 1: Recepción de señal HDB3

1. Regular el osciloscopio para la observación de las señalizaciones PCM 0–5 volts a 2048Kbps. Esto es 500mV V/Div y 250ms T/Div



2. Poner la sonda de prueba con escala 10:1 y conectar una de ellas a TP32 y Tierra, y la otra sonda a TP33 y tierra.
3. Seleccionar diferentes ranuras de tiempo (Time Slot) y fijarla en la ranura 1.
4. Compare la señalización HDB3 antes y después de la conversión de señal bipolar (TP32) y en unipolar (TP33).
5. Para visualizar con mayor claridad la imagen haga una captura de pantalla con el botón RUN/STOP del osciloscopio y luego varíe el T/Div.
6. Guarde la señal capturada en su memoria USB y anote los datos más relevantes que observe en dicha señal.
7. Presione nuevamente el botón RUN/STOP para continuar con la visualización normal de la señal.
8. Desplazar la sonda de TP32 a TP38. Detectar la relación de fase entre los impulsos HDB3 y la señal de reloj regenerada por el receptor.
9. Desplace las sondas a TP33 y TP37, detecte las relaciones de fase entre los impulsos HDB3 y las componentes de recepción RxA y RxB, las transiciones negativas de estas componentes localizan los instantes de muestreo de los impulsos.
10. Desplace la sonda de TP33 a TP 36 y observe ambas señales que corresponden a la codificación unipolar de HDB3.

Actividad 2: Recepción de señal HDB3 ante una llamada telefónica.

1. Establecer una llamada telefónica entre los teléfonos 1 y 2.
2. Realice los mismos pasos de la actividad 1.

VII. Preguntas de control

1. ¿Cómo se regenera la señal en el receptor?
2. ¿Qué frecuencia es utilizada para reconstruir la señal en TP38?



-
3. ¿Qué sucede con la señalización cuando se realiza una llamada telefonica?
 4. ¿Cómo es la relación de fase entre la señal HDB3 y la señal regenerada?



Laboratorio No. 8: Selección de ranuras de tiempo en una llamada telefónica

Curso	Capacitación en telefonía IP		
Modulo	Redes de Telefonía	Grupo	
Tipo Practica	<input type="checkbox"/> Laboratorio <input type="checkbox"/> Simulación		
Unidad Temática			
No Alumnos por practica	1	Fecha	
Nombre del Profesor			
Nombre(s) del Alumno(s)			
Tiempo estimado	45 minutos	Vo. Bo. Del Docente	
Comentarios			

Objetivos de la práctica de laboratorio

I. Objetivo General

1. Observar las ranuras de tiempo (Time Slot o Trama) PCM de transmisión y recepción que forman los circuitos de telefonía.

II. Objetivos específicos

1. Identificar en que trama o ranura de tiempo se está transmitiendo los datos de una llamada.
2. Observar el comportamiento de los datos transmitidos durante una llamada telefónica.
3. Mostrar cómo se transmiten las tramas en canales distintos.

III. Medios a utilizar

- Unidad EE-PM
- 4 Teléfonos del Equipo
- Osciloscopio



IV. Introducción

Este laboratorio consiste en seleccionar y observar las tramas o ranuras de tiempo (Time Slot) PCM de transmisión y recepción que forman los circuitos de voz.

En la línea PCM de transmisión (PCM TX) las ranuras de tiempo ocupadas son las son cuatro de 32:

- Ranura de tiempo 1 para el teléfono #1
- Ranura de tiempo 2 para el teléfono #2
- Ranura de tiempo 3 para el teléfono #3
- Ranura de tiempo 4 para el teléfono #4

En la línea PCM de recepción (PCM RX) todas las ranuras de tiempo tienen el valor PCM “0”, en reposo (se alternan “1” y “0”, según la codificación ADI: Alternate Digit Inversion = inversión alternada de marcas).

Cuando se establece uno o más circuitos de voz, los datos de recepción aparecen en las siguientes ranuras de tiempo (Tramas).

- Ranura de tiempo 17 para el teléfono #1
- Ranura de tiempo 18 para el teléfono #2
- Ranura de tiempo 19 para el teléfono #3
- Ranura de tiempo 20 para el teléfono #4

V. Conocimientos previos

- Multiplexación de canales
- Sistemas de portadoras E1

VI. Procedimiento

El escenario a implantarse se muestra en la Figura 3. Aquí se presentan los medios a utilizar como son el equipo PCM/EEPM, los teléfonos y el osciloscopio:

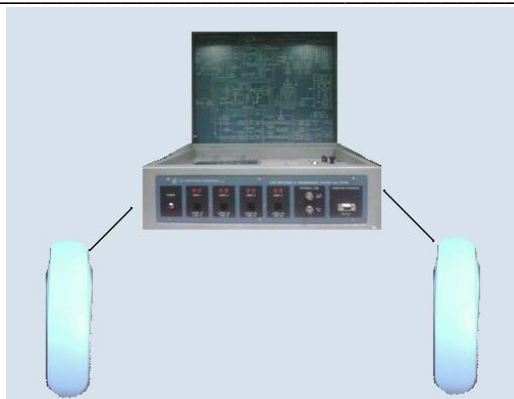


Figura 4 Escenario a implementar

Actividad 1: Selección de ranuras de tiempo

11. Regular el osciloscopio para la observación de las señalizaciones PCM 0–5 volts a 2048Kbps. Esto es 500mV V/Div y 250ms T/Div
12. Poner las sonda de prueba con escala 10:1 y conectar una de ellas a TP19 y Tierra (Tx, trama PCM en transmisión) y la otra a TP22 y tierra (Rx, trama PCM en recepción).
13. Observe las señales que se están registrando.
14. Mediante el selector de décadas del panel frontal (TIME SLOT SELECTION) identificar los canales de transmisión de la línea Tx, reconocibles por los demás canales (no utilizados) por la presencia de códigos pcm cercanos de cero (alternativa de unos y ceros).
15. Los canales de recepción (línea Rx) no son reconocibles entre sí, ya que en reposo todos tienen el valor PCM "0".
16. Para visualizar con mayor claridad la imagen haga una captura de pantalla con el botón RUN/STOP del osciloscopio y luego varié el T/Div.
17. Guarde la señal capturada en su memoria USB y anote los datos más relevantes que observe en dicha señal.
18. Presione nuevamente el botón RUN/STOP para continuar con la visualización normal de la señal.



19. Realice llamadas entre dos teléfonos, por ejemplo el #2 y el #4, y sincronizar el osciloscopio antes en el Time Slot 2 (seleccionar 2 en el panel frontal) y luego en el Time Slot 4 (seleccionar 4). Observar que en presencia de voz los canales de transmisión (2 y 4) asumen códigos variables
20. Capture la imagen con el osciloscopio, ajuste T/div y V/div para observar con claridad la imagen.
21. Sin colgar los teléfono 2 y 4, seleccione la ranura de tiempo 18 y 20 ya que en ellos se muestran los datos de voz recibidos en los teléfonos interconectados actualmente. Estos códigos son variables con respecto a las configuraciones fijas de los ceros PCM que están presentes en los demás canales que no se están utilizando.
22. Conectando dos teléfonos cercanos, por ejemplo el #2 y el #3, se pueden acercar suficientemente los respectivos "Time Slots" de transmisión y recepción de modo que se puedan observar simultáneamente en el osciloscopio, como se muestra en la Figura 5.
23. En este caso, si se habla en uno de los dos teléfonos (por ejemplo, el #2) se observarán las variaciones del relativo canal de transmisión (Time Slot #2) que se repercuten en el canal de recepción del teléfono #3 (Time Slot #19), y viceversa.
24. Repetir la prueba con conexiones diferentes, también simultáneas.

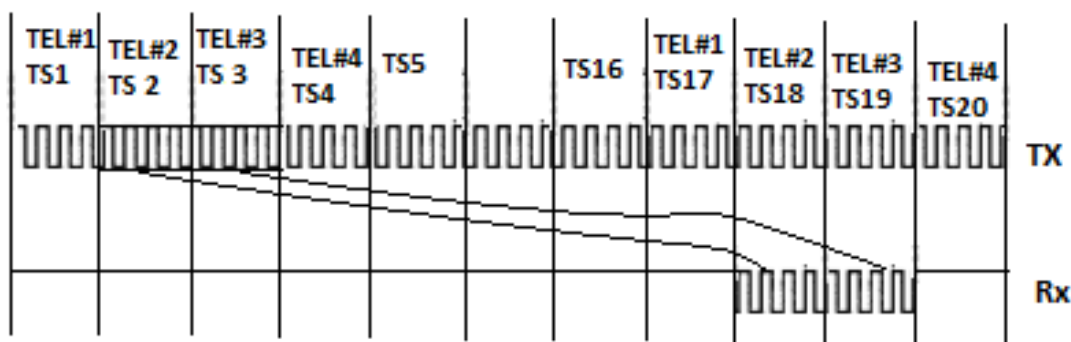


Figura 5 Tramas de Transmisión y recepción



VII. Preguntas de control

1. ¿Qué es una Trama?
2. ¿Cuántos bits posee una trama?
3. ¿Por qué las tramas de recepción permanecen en nivel alto mientras no existe comunicación entre dos teléfonos?
4. ¿Son los pulsos de las señales de transmisión y recepción las mismas?



Laboratorio No. 9: Fases de una conexión Telefónica. *

Modulo	Redes de Telefonía		
Tipo Práctica	<input type="checkbox"/> Laboratorio <input type="checkbox"/> Simulación		
Unidad Temática			
No Alumnos por práctica	2	Fecha	
Nombre del Profesor			
Nombre(s) de Alumno(s)			
Tiempo estimado		Vo. Bo. Del Profesor	
Comentarios			

Objetivos de la práctica de laboratorio

I. Objetivo general

1. Seguir las fases de ocupación y liberación en una conexión telefónica entre dos teléfonos.

II. Objetivos específicos

1. Analizar la actividad de la central cuando se ocupa la línea
2. Detectar las secuencias de impulsos de apertura la línea de usuario
3. Observar el comportamiento de la señalización multifrecuencia.
4. Verificar la realización y liberación de una conexión.

III. Medios a utilizar

- Unidad PCM/EV
- Teléfonos del equipo
- Osciloscopio
- Multímetro
- Memoria USB

IV. Introducción

En este laboratorio se analiza la actividad realizada por la central después de la ocupación de una línea tales como el cierre del loop de usuario.



El loop de usuario determina la transición en el estado activo de la señal del interfaz de usuario, por tanto cuando se descuelga uno de los teléfonos conectados a este equipo, el terminal ocupa la línea es decir línea se cierra la línea de usuario en los circuitos de fonía y en respuesta a la ocupación de la línea, la central envía al teléfono el tono de **invitación a discar** el cual es un tono de frecuencia de 425 Hz, adecuadamente modulado **on/off** en **tono/pausa/tono/pausa**. De esta manera la central le señaliza al usuario la propia disponibilidad a la conexión (disponibilidad de línea).

También se analiza la detección de las secuencias de impulsos de apertura de la línea debidas al discado decádico, es decir el envío a la central de una señalización adecuada que identifica el número de línea del teléfono solicitado en conexión.

Existen dos clases de señalizaciones de discado: dedicada y de multifrecuencia. A cada impulso de apertura le corresponde una transición de reposo de la señal de línea suministrada por el interfaz de usuario.

La unidad de control cuenta estas transiciones para remontar a las cifras transmitidas, evalúa la duración de las pausas entre cada cifra durante el cierre y adquiere el número de selección con el cual procede a la construcción de la conexión requerida

Cuando se observa el comportamiento de la señalización multifrecuencia en la cual las cifras de selección están codificadas mediante parejas de tonos acústicos por el interfaz de usuario.

Finalmente en esta práctica se estudia el circuito de decodificación del módulo el cual suministra el valor de las cifras transmitidas como códigos binarios de 4 bits, más una línea de dato valido; los códigos binarios son visualizados mediante LED.

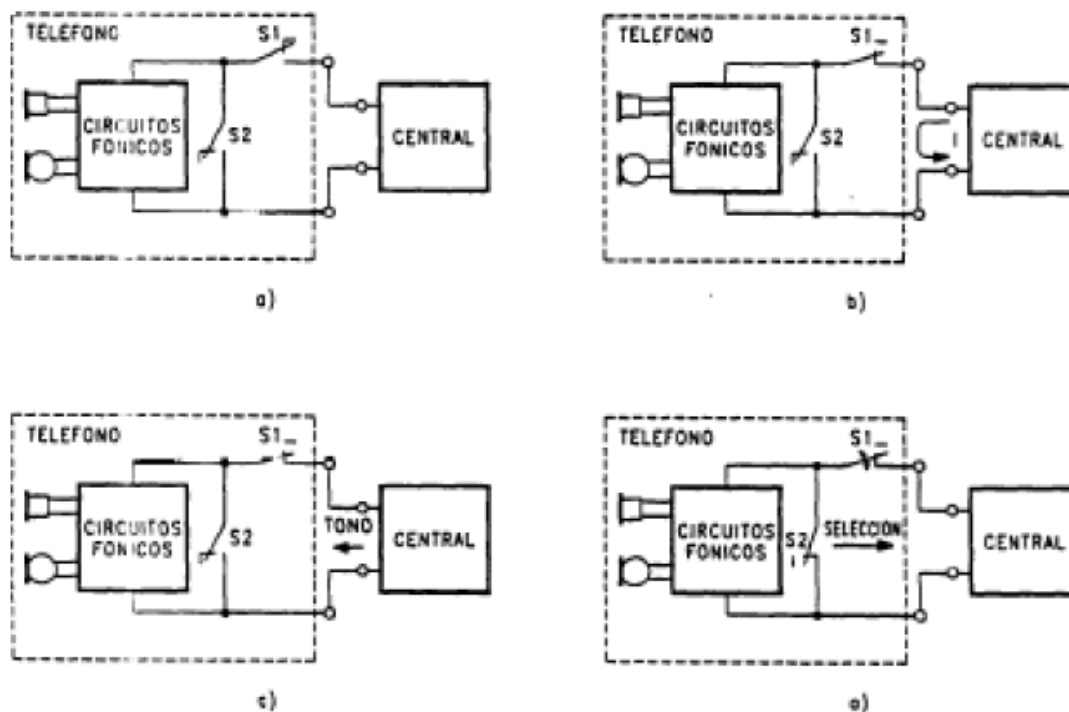


Fig. 1 a. línea de reposo b. ocupación de la línea c. envío del tono de invitación a discar d. discado.

V. Conocimientos previos

- Conexión entre el Teléfono y la Central Telefónica.
- Marcación por pulso o Decadico.
- Marcación por tonos o DTMF.
- Establecimiento de una llamada.

VI. Procedimiento

El escenario a implantarse se muestra en la figura 1. Aquí se presentan los medios a utilizar como son el equipo PCM/EV y los teléfonos:

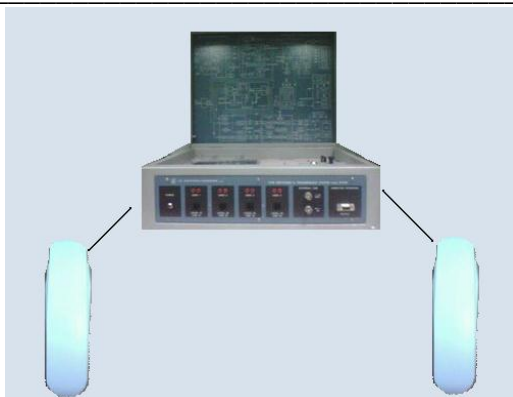


Fig. 2 Escenario de laboratorio.

Actividad 1: Ajuste de parámetros.

1. Conecte el módulo PCM/EV al suministro eléctrico y oprima el Switch de encendido/apagado.
2. Conecte los 4 teléfonos a los bornes de línea del panel del modulo.
3. Verifique que los teléfonos están en modo Decadico (pulso), si no es así cámbielo a dicho modo.
4. Verifique que todos los LED de visualización de las alimentaciones y el LED Test Mode estén encendidos.
5. Conecte un multímetro entre TP13 y TP12 para medir la tensión de línea correspondiente al teléfono #1 (User 1), podrá observar que la tensión de línea tiene un valor de 40V.
6. Mantenga el multímetro conectado a los TP13 y TP12. Levante el teléfono #1 (User 1) y observe el cambio de tensión de línea, que será aproximadamente de 10 v por efecto del cierre del lazo de usuario de la impedancia en continua del teléfono. Este estado también es señalado por el led Dial en el panel Display en Line Signaling.

Actividad 2: Invitación a marcar

1. Conectar una sonda del osciloscopio entre TPI3 y tierra



2. Levante el teléfono #1 (User 1) y regule las escalas en el osciloscopio para que pueda observar la señal correspondiente al tono de invitación a marcar. Este mismo tono se puede observar entre TP15 y tierra, debido a que esta es la entrada al interfaz de usuario (RECEIVE INPUT).
3. Guarde la señal en su memoria USB y anote los resultados obtenidos.
4. Cuelgue el teléfono.
5. Conecte una sonda del osciloscopio a TP17 y a tierra, asegúrese que la escala V/Div. en el osciloscopio se encuentre a 500mV/Div y Time/Div a 100mSeg/Div. Observe la señal
6. Levante el teléfono #1(User 1) y observe como la señal cambia a cero debido a que TP17 corresponde a la señal de línea ocupada (Switch Hook Detector) del interfaz usuario y su estado lógico activo es "0", el cual también está señalizado mediante LED User 1.
7. Marque una cifra y observe que el tono de invitación a marcar no se escucha más.
8. En el osciloscopio se observarán las transiciones de estado debidas a la marcación dedicada (impulsos de apertura de la línea).
9. Marque otra cifra en el teléfono #1 regulando la escala de los tiempos del osciloscopio de modo que se puedan ver las duraciones de los impulsos y las pausas cuando el teléfono está llamando. En base a las cifras seleccionadas, el teléfono puede recibir el tono de ocupado o el tono de libre, junto con la señal de llamada en uno de los restantes teléfonos.
10. Cuelgue el teléfono, levántelo nuevamente y presione un número. Realice una captura de la señal obtenida mientras presiona dicho numero (Presione el botón RUN/STOP del osciloscopio).
11. Guarde la señal capturada en su memoria USB



-
12. Presione nuevamente el botón RUN/STOP para continuar con la visualización normal de la señal.
 13. Cuelgue el teléfono y observe en el osciloscopio el retorno de la línea de ocupado (Switch Hook Detector) a reposo (nivel alto).

Actividad 3: Marcación

1. Cambie los teléfonos a modo DTMF.
2. Conecte una sonda del osciloscopio en TP16 y tierra.
3. Ajuste las escalas del V/Div. del osciloscopio a 2 V/Div, Time/Div a 1mSeg/Div, y la sonda de prueba a 1:1.
4. Si la señal no se observa ajuste la posición con el osciloscopio hasta que logre visualizarla.
5. Levante el teléfono #1(User 1).
6. Observe el encendido del LED User 1 conectado con la línea de ocupado (Switch Hook Detector) del interfaz usuario. Después de haber escuchado el tono de invitación a marcar, digite una cifra y observe nuevamente la desaparición del tono de invitación a marcar y la presencia de una señal en el osciloscopio.
7. Marque otra cifra y regule nuevamente la escala de los tiempos en el osciloscopio de modo que se optimice la observación de los tonos DTMF. Esta señal que se observa en TP16 es la suma de los dos tonos, alto y bajo, que codifican la cifra de selección.
8. Realice una captura de la señal obtenida mientras presiona un número del teléfono (Presione el botón RUN/STOP del osciloscopio).
9. Guarde la señal capturada en su memoria USB
10. Presione nuevamente el botón RUN/STOP para continuar con la visualización normal de la señal.



11. En la figura 3 se observa una tabla correspondiente al código DTMF en dependencia de lo que se marca en el teléfono. En base a las cifras de selección, el teléfono puede recibir el tono de ocupado o el tono de libre, junto con la señal de llamada en uno de los restantes teléfonos.

Q1	Q2	Q3	Q4	CIFRA:
ON	OFF	OFF	OFF	1
OFF	ON	OFF	OFF	2
ON	ON	OFF	OFF	3
OFF	OFF	ON	OFF	4
ON	OFF	ON	OFF	5
OFF	ON	ON	OFF	6
ON	ON	ON	OFF	7
OFF	OFF	OFF	ON	8
ON	OFF	OFF	ON	9
OFF	ON	OFF	ON	0

Fig. 3. Código de marcación DTMF

12. Cuelgue el teléfono y observe el apagado del LED de línea ocupada.
13. Conecte una de las sonda del osciloscopio a TP12 (correspondiente al RING) y a tierra y ajuste las escalas V/Div a 5V/Div y a la del Time/Div a 500ms/Div.
14. Conecte la otra sonda a TP14 (correspondiente al Relay Driver) y tierra, ajustando las escalas V/Div a 1 V/Div y la del T/Div a 500ms/Div.
15. Verifique que ambas sondas estén en 10:1.
16. Desde un teléfono diferente del #1(User 1). marque después de escuchar el tono de invitación a disar, el número del teléfono #1 (User 1). Cuando llega la señal de llamada al teléfono #1, en TP12 se visualiza la señal de la llamada de aproximadamente 15 Vpp y en TP14 el nivel se reduce a cero.
17. Observe la correspondencia entre el estado de la línea de llamada, la activación del relé junto con el encendido del LED de llamada, la presencia de la corriente en línea y el tono de libre enviado al teléfono llamante. Todas estas



señalizaciones tienen la misma temporización correspondiente a un segundo de actividad cada cinco segundos.

18. Realice una captura de la señal obtenida mientras se encuentre repicando el teléfono #1 (User 1). (Presione el botón RUN/STOP del osciloscopio).
19. Guarde la señal capturada en su memoria USB
20. Presione nuevamente el botón RUN/STOP para continuar con la visualización normal de la señal.
21. Cuando se levanta el teléfono #1 (User 1). se enciende el LED de línea ocupada e instantáneamente se interrumpe la corriente de llamada, debida al interfaz de usuario. Inmediatamente después, la unidad de control suprime el comando de llamada y el tono de libre del teléfono llamante.
22. Levante el teléfono y en este instante se establece la conexión entre los dos.

Actividad 4: Control de la conexión entre los teléfonos

1. Levante el teléfono # 1 (User 1) y llame a otro teléfono.
2. Levante el teléfono al que llamo y verifique que la conexión se ha establecido
3. Cuelgue el teléfono que recibió la llamada, sin colgar el teléfono que la inicio.
4. Levante de nuevo el teléfono que colgó y observe la permanencia de la conexión entre los teléfonos.
5. Cuelgue el teléfono llamante observando la liberación de la conexión.

Actividad 5: Señal de ocupado.

1. Conectar una sonda del osciloscopio a TP15 y tierra, ajustando las escalas de tiempo a 2.5 ms/Div y de voltaje a 50mv/Div con la sonda en 10:1
2. Descuelgue el teléfono #2 (User 2). y observe el encendido del LED que indica la presencia del tono de invitación a marcar.
3. Deje descolgado el teléfono #2 (User 2).



4. Levante el teléfono #1 (User 1). y llame al teléfono #2 (User 2). Observe el encendido del LED que indica presencia del tono de línea ocupada en el teléfono #1 (User 1).
5. Examine las características del tono regulando de manera adecuada las escalas del osciloscopio.
6. Cuelgue los teléfonos y llame desde el teléfono #1 (User 1) a cualquiera de los otros teléfonos. Espere la señal de llamada en el teléfono seleccionado y el encendido del LED de presencia del tono de libre en el teléfono #1 (User 1).
7. Examine las características del tono regulando de manera adecuada las escalas del osciloscopio.
8. Descuelgue el teléfono llamado y verifique la presencia de la conexión entre ambos teléfonos.
9. Cuelgue de nuevo los teléfonos.

VII. Preguntas de control

1. ¿Por qué la tensión de línea existente entre TP12 y TP13 pasa de 40V a 10V cuando se levanta el teléfono #1 (User 1)?
2. ¿Cuánto es la frecuencia de la señal que se observa en el osciloscopio en TP13 cuando el teléfono replica?
3. ¿Cuándo trabaja con los teléfonos en modo DTMF que código se ve en el panel DTMF cuando levanta el teléfono #1 (User 1) y llama al teléfono #2 (User 2)? ¿cumple con la tabla mostrada en la figura 3?
4. ¿Cuál es la señalización que utilizan las centrales de la PSTN?
5. ¿Cuál es el procedimiento para realizar una llamada en la PSTN?



Laboratorio No. 10: Tensiones y señales de control

Modulo	Redes de Telefonía		
Tipo Práctica	<input type="checkbox"/> Laboratorio <input type="checkbox"/> Simulación		
Unidad Temática			
No Alumnos por práctica	2	Fecha	
Nombre del Profesor			
Nombre(s) de Alumno(s)			
Tiempo estimado		Vo. Bo. Del Profesor	
Comentarios			

Objetivos de la práctica de laboratorio

I. Objetivo general

1. Observar el código de línea transmitido en una llamada telefónica.

II. Objetivos específicos

1. Visualizar como los componentes de polaridad de la señal HDB3 separado en líneas distintas.
2. Comprender como se atenúa una señal en una línea.

III. Medios a utilizar

- Unidad EE-PM con teléfonos
- Osciloscopio

IV. Introducción

La finalidad de este ejercicio es la de poner en evidencia el proceso de codificación HDB3 en la señalización saliente. El interfaz suministra al transmisor de línea las dos componentes de polaridad de la señal HDB3, separadas en líneas distintas TXA y TXB, con la misma polaridad positiva. En la salida del transmisor está presente la señal HDB3 compuesta. Para analizar la codificación HDB3 en los datos de sincronismo, la señalización y canales de voz que constituyen las tramas del sistema primario, habrá que

tener presente que: en el intervalo temporal 0 se alternan configuraciones de alineación (tramas pares) con configuraciones de no alineación (tramas Impares); en el intervalo temporal 16 los datos de señalización son fijos, en el caso del sistema didáctico analizado, salvo su sustitución con la alineación de multitrama una vez cada 16 tramas; los datos de voz son variables por naturaleza y es suficiente el cambio de un solo bit en los canales de voz para cambiar la configuración de todos los impulsos sucesivos. El caso más favorable se refiere a los canales de transmisión utilizados que son recibidos como secuencias bits todos iguales a "1"; por ello, es más fácil observar la ley alternancia incluida en la codificación HDB3. Por ejemplo, para los canales 17-31 y en situación de secuencias predominantes de las componentes TXA y TXB, así la configuración de la señal HDB3 son las que se muestran en la Figura 1. Observar en el osciloscopio las secuencias de la figura con las fases en parte superpuestas, pero con un caso predominante sobre los demás.

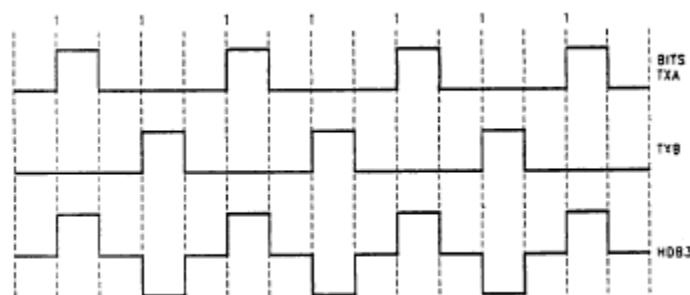


Figura 6 Código HDB3

V. Procedimiento

El escenario a implantarse se muestra en la Figura 2. Aquí se presentan los medios a utilizar como son el equipo PCM/EEPM, los teléfonos y el osciloscopio:

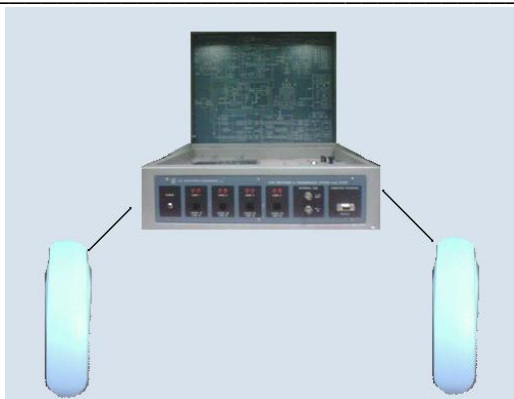


Figura 7 Escenario a usar

Actividad 1: Códigos de líneas HDB3 en telefonía.

1. Ajuste el módulo PCM-EEPM en MODO TEST, para ello diríjase al panel de control de selección y ubique el switch en modo local y luego presione el push botón (MODO SELECT) para cambiar a MODE TEST. Confirme dicho modo con el led rojo q se encenderá en panel.
2. Conecte dos sondas de pruebas al osciloscopio.
3. Conecte una de las sondas del osciloscopio a TP27 y a tierra y la otra sonda a TP28 y tierra asegurándose primero que los parámetros Noise y Attenuation del módulo PCM se encuentren en cero.
4. Observe las señales mostradas y ajuste las escalas del osciloscopio 200mV/Div y 500nsegT/Div para observar con mayor claridad las señales.
5. Para visualizar con mayor claridad la imagen haga una captura de pantalla con el botón RUN/STOP del osciloscopio y luego varié el T/Div.
6. Guarde la señal capturada en su memoria USB y anote los datos más relevantes que observe en dicha señal.
7. Presione nuevamente el botón RUN/STOP para continuar con la visualización normal de la señal.



8. Varié las ranuras de tiempo pulsando sobre los puch botón desde 0 hasta 31, haga énfasis en las ranuras 1,2,3,4 observe y anote los resultados visualizados del comportamiento de la señal.
9. Una vez que observo las señales en TP27 y TP28 con los parámetros Noise y Attenuation en cero, desplace de manera intermitente la sonda de TP27 en TP30.
10. Haga una captura de pantalla con el botón RUN/STOP del osciloscopio y luego varié el T/Div.
11. Guarde la señal capturada en su memoria USB y anote los datos más relevantes que observo en dicha señal.
12. Presione nuevamente el botón RUN/STOP para continuar con la visualización normal de la señal.
13. Desplace la sonda de prueba alternativamente la sonda ubicada en TP28 en TP30.
14. Capture la imagen y guarde la señal capturada en su memoria USB, anote los datos más relevantes que observo en dicha señal.
15. Presione nuevamente el botón RUN/STOP para continuar con la visualización normal de la señal.
16. Varié los potenciómetros de RUIDO y ATENUACION, observe y anote los resultados.

Actividad 2: Códigos de líneas HDB3 durante una llamada.

1. Levante el teléfono número 2 y marque al teléfono 3.
2. Realice todo el procedimiento realizado en la actividad 1, manteniendo la llamada entre los teléfonos 2 y 3, y haciendo énfasis en las ranuras de Tiempo 2 y 3.
3. Anote las diferencias encontradas.



VI. Preguntas de control

1. ¿Qué es HDB3?
2. ¿Qué sucede cuando en la transmisión de datos existen más de 4 ceros consecutivos?
3. ¿Qué sucede con la señal HDB3 cuando se varían los potenciómetros de Atenuación y Ruido.
4. ¿Qué sucede con los componentes TXA y TXB cuando se observa TP30?

Guías Prácticas del Módulo II: Redes de Datos



Laboratorio No. 1: Introducción al simulador de redes.

Curso	Capacitación en telefonía IP		
Modulo	Redes de Datos	Grupo	
Tipo Practica	<input type="checkbox"/> Laboratorio <input type="checkbox"/> Simulación		
Unidad Temática			
No Alumnos por practica	1	Fecha	
Nombre del Profesor			
Nombre(s) del Alumno(s)			
Tiempo estimado	60 minutos	Vo. Bo. Del Docente	
Comentarios			

Objetivos de la práctica de laboratorio

I. Objetivo General

1. Adquirir conocimiento básico en el uso del simulador de redes.

II. Objetivos específicos

1. Conocer los elementos y facilidades brindadas por el simulador.
2. Identificar los tipos de líneas utilizadas para interconectar los dispositivos.

III. Medios a utilizar

- Equipo de cómputo
- Programa simulador de redes IP

IV. Introducción

Packet Tracer es la herramienta de aprendizaje y simulación de redes interactiva. Esta herramienta les permite a los usuarios crear topologías de red, configurar dispositivos, insertar paquetes y simular una red con múltiples representaciones visuales.

En este programa se crea la topología física de la red simplemente arrastrando los dispositivos a la pantalla. Luego clickando en ellos se puede ingresar a sus consolas de configuración. Allí están soportados todos los comandos del Cisco OS e incluso funciona el "tab completion". Una vez completada la configuración física



y lógica de la red, también se puede hacer simulaciones de conectividad (pings, traceroutes, etc) todo ello desde las mismas consolas incluidas.

V. Conocimientos previos

- Dispositivos de red
- Topologías lógicas de redes IP
- Topologías físicas de redes IP

VI. Procedimiento

Actividad 1: Reconocimiento de los elementos y barras de Packet tracer

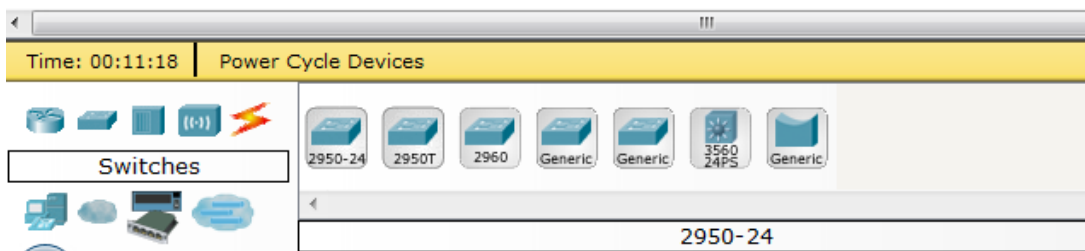
Packet tracer presenta una serie de dispositivos de la marca Cisco. Todos estos elementos se encuentran en la parte inferior de la pantalla de inicio. La Figura. 1 nos muestra la ubicación de estos dispositivos en la barra de herramientas del programa.



Figura. 1

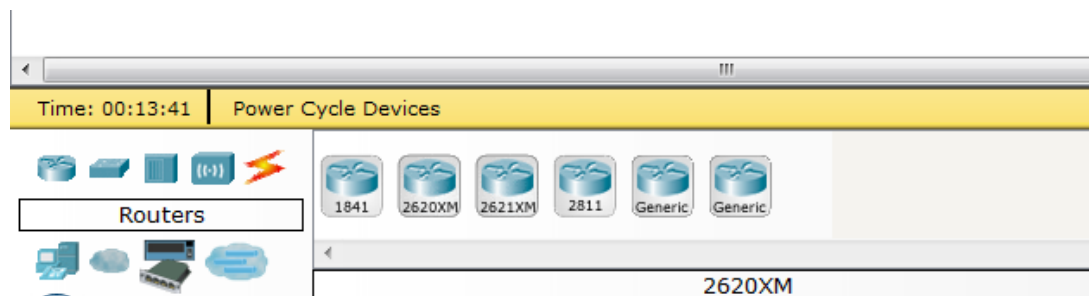
Algunos de los dispositivos que se presenta son:

Switches

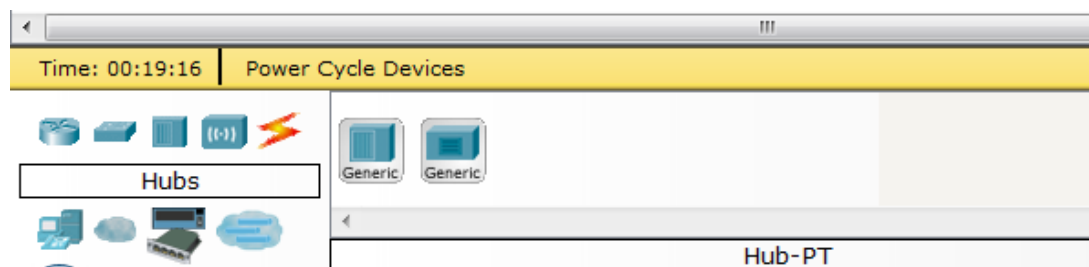




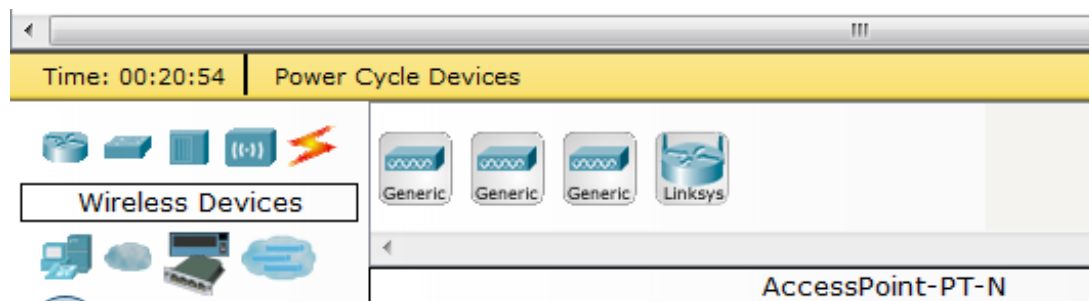
Routers



Hubs

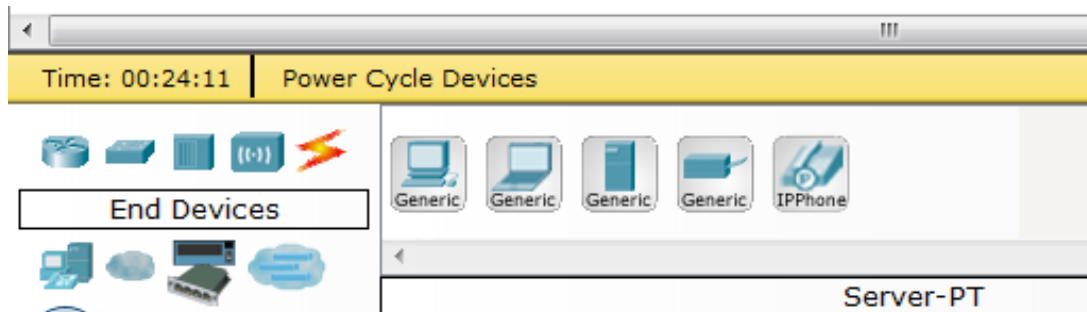


Dispositivos inalámbricos

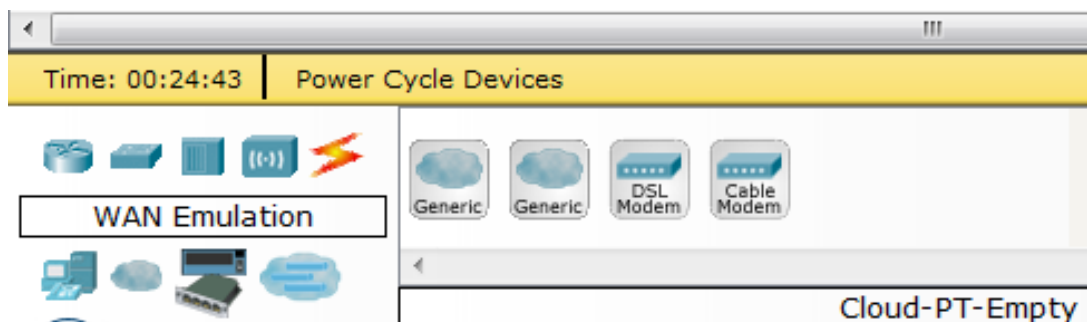




Dispositivos Finales - Hosts



Emulación de WAN



Actividad 2: Interconexión de dispositivos

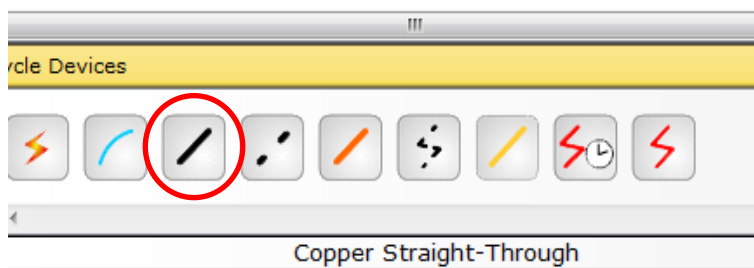
1. Tome el icono de computadora y arrástrelo hasta el área de trabajo en la pantalla principal.
2. Tome el icono de router y arrástrelo hasta el área de trabajo.
3. Observe en el panel de herramientas los distintos tipos de cables para interconectar los dispositivos.

Cable de consola



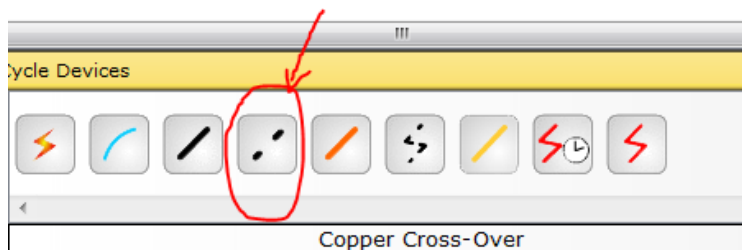
Este tipo de cable se utiliza para conectar un router o un switch a una computadora con el fin de ingresar a la CLI (línea de comandos) interna del router o switch, para programarlo.

Cable de cobre configuración de línea directa.



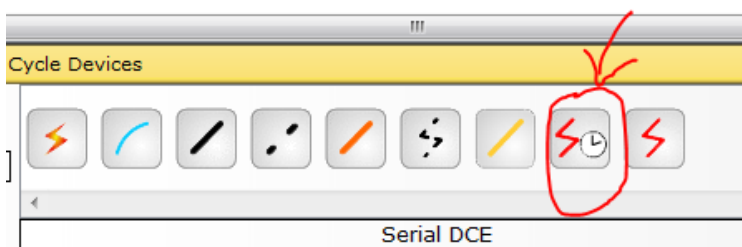
Este cable se utiliza para interconectar dispositivos diferentes. El cable se conecta a los puertos int 0/0 o int0/1 de Ethernet. Ejemplo de estas conexiones son: switches con router, y computadoras y switches.

Cable de cobre configuración de línea cruzada.



Este tipo de cable se utiliza para interconectar dispositivos iguales en los puertos Ethernet int0/0 e int0/1. La conexión entre switches o computadoras.

Cable serial DCE



Este tipo de cable se utiliza para la interconexión de routers. El cable se conecta al extremo de la conexión que definirá la tasa de transferencia de datos que se usará en el enlace.

Cable serial DTE



Este cable se usa junto con el cable DCE, en este caso se emplea en el otro extremo de la conexión entre dos routers que no controla la velocidad de transferencia.

4. Conecte el router a la computadora con el cable correcto.
5. En la Figura. 2 se muestran una serie de posibles interconexiones. Realice cada interconexión de la figura en el simulador.

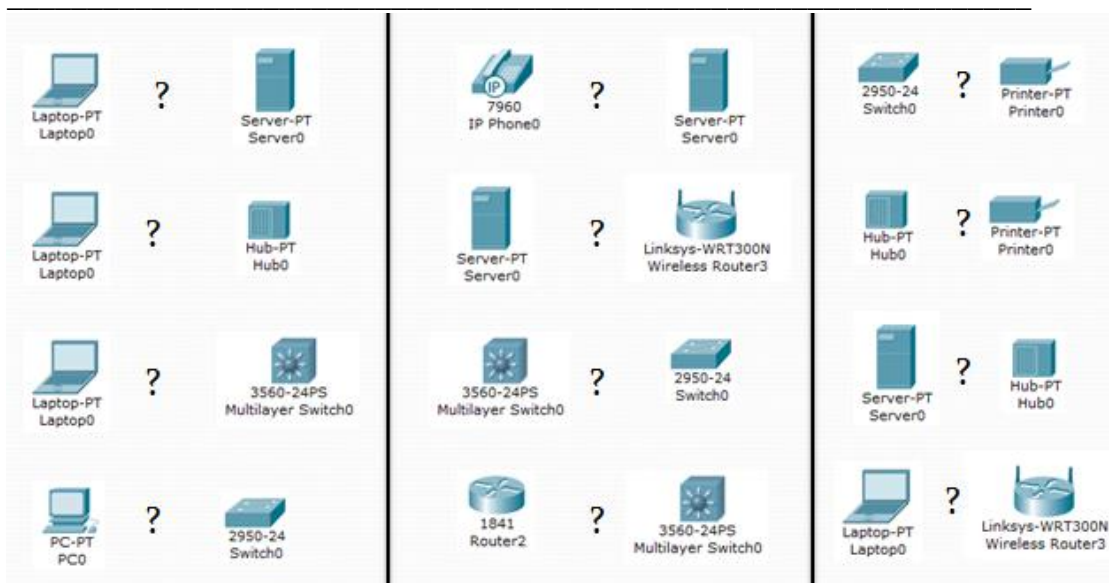
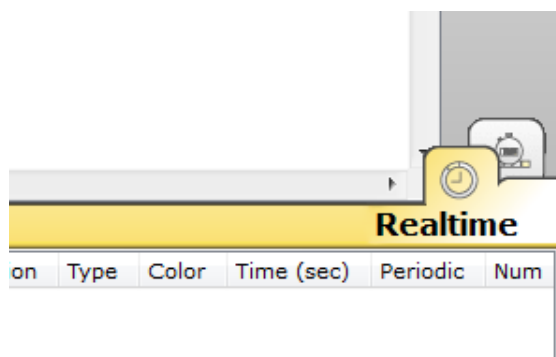


Figura. 2

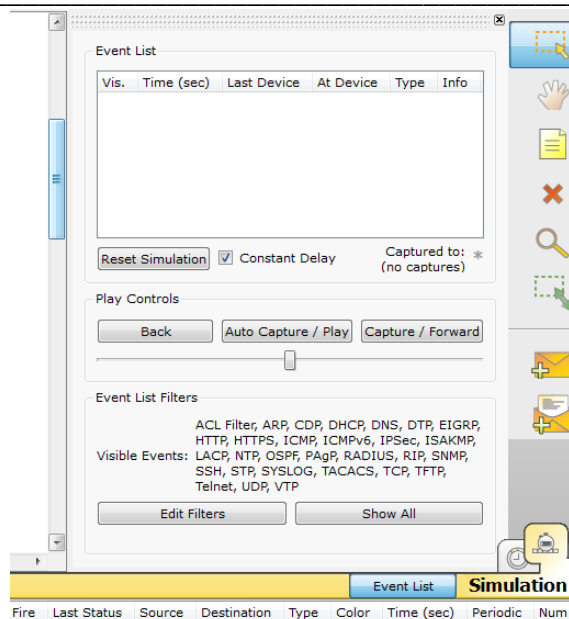
Modo en tiempo real



El modo en tiempo real permite a los usuarios el observar el comportamiento en tiempo real de la red que se diseña.

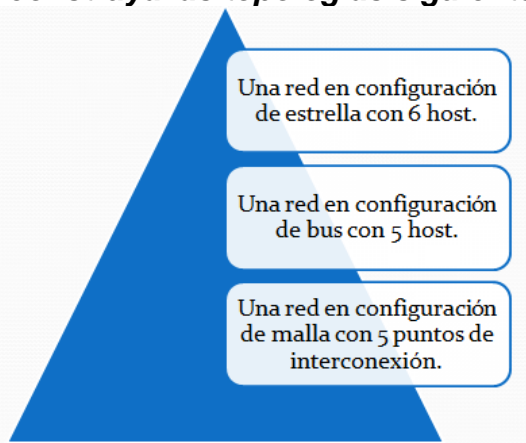
Este proceso permite agilizar el proceso de análisis y detectar errores que pueden surgir a medida que la red opera.

Modo simulación



A través de este modo el usuario puede observar el envío detallado de cada paquete y seguir la trayectoria de este hasta que llegue a su destino o no. La ventana de simulación nos permite generar un filtrado de los paquetes que nos interesan ver.

Actividad 2: Diseñe y construya las topologías siguientes en el simulador.





Actividad 3: Elabore un cuadro comparativo sobre las topologías de la actividad anterior.

Esquema de red	Dispositivos utilizados	Ventajas	Desventajas	Consideraciones
Bus				
Estrella				
Malla				

Actividad 4: Complete y construya la red mostrada en la Figura. 3

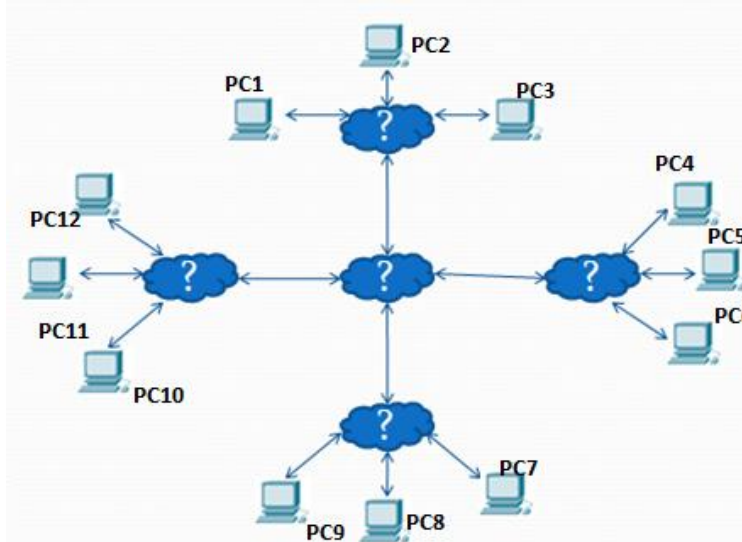


Figura. 3

1. Sustituya el símbolo de “?” por el dispositivo correcto.
2. Utilice las direcciones IP desde 192.168.0.1 hasta 192.168.0.12 para configurar las PC a como se muestra en la siguiente tabla.

PC1 – 192.168.0.1	PC7 – 192.168.0.7
PC2 – 192.168.0.2	PC8 – 192.168.0.8
PC3 – 192.168.0.3	PC9 – 192.168.0.9
PC4 – 192.168.0.4	PC10 – 192.168.0.10
PC5 – 192.168.0.5	PC11 – 192.168.0.11



PC6 – 192.168.0.6

PC12 – 192.168.0.12

3. Para configurar las direcciones IP de las PC

- De doble click sobre la PC que desea configurar.
- Dirijase a la pestaña de configuraciones y luego a la Opcion de Interface FastEthernet. Ver figura 4
- Escriba la dirección IP de la PC y mascara de red.
- Cierre la ventana.

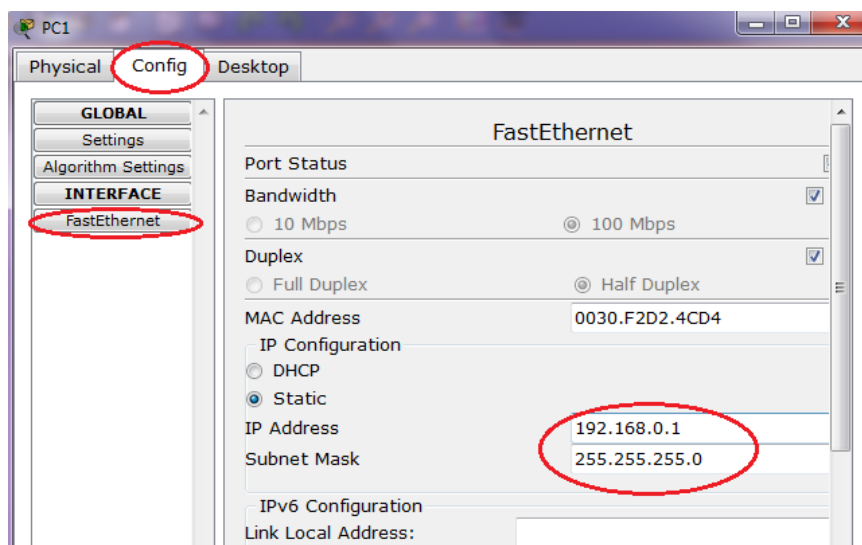


Figura. 4

4. Envié un paquete de prueba desde una PC a otra para comprobar su funcionamiento.

- De click sobre la PC.
- Dirijase a la pestaña Desktop y luego a la opción Command Prompt. Ver Figura.5



Figura. 5

- Envíe el paquete de prueba con el comando "ping [dirección ip de PC destino]".ver Figura .6

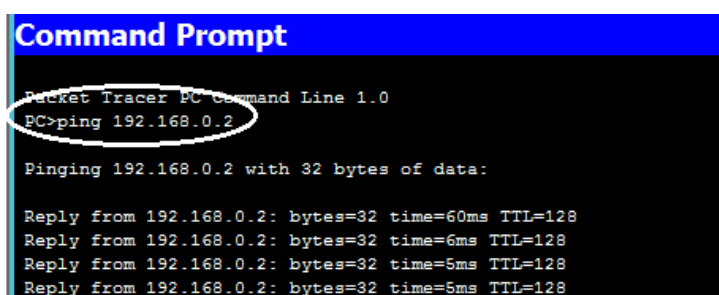


Figura. 5

5. Si en el paso anterior utilizo Hub entonces sustitúyalos por switches para la interconexión de los dispositivos.
6. Envié un paquete de prueba desde una PC a otra para comprobar su funcionamiento.

VII. Preguntas de control

1. En la última actividad, ¿qué dispositivos utilizo? ¿Por qué?
2. Que desventajas observo en el esquema de la actividad 3.
3. ¿Qué ventajas posee el empleo de switches en lugar de hubs?
4. ¿Cuál es la diferencia entre los cables DTE y DCE?
5. ¿Cuáles son las ventajas del simulador de redes?



6. ¿Qué cable utilizaría para conectar un switch a un router?
7. ¿Qué cable utilizaría para conectar una computadora a un router?



Laboratorio No. 2: Introducción a Wireshark

Curso	Capacitación en telefonía IP		
Modulo	Redes de Datos	Grupo	
Tipo Practica	<input type="checkbox"/> Laboratorio <input type="checkbox"/> Simulación		
Unidad Temática			
No Alumnos por practica	1	Fecha	
Nombre del Profesor			
Nombre(s) del Alumno(s)			
Tiempo estimado	75 minutos	Vo. Bo. Del Docente	
Comentarios			

Objetivos de la práctica de laboratorio

I. Objetivo General

1. Adquirir conocimiento básico en el uso del analizador de protocolos

II. Objetivos específicos

1. Conocer las funciones y herramientas brindadas por el analizador.
2. Identificar los tipos de protocolos que se pueden analizar con wireshark.

III. Medios a utilizar

- Equipo de cómputo
- Analizador de protocolos Wireshark

IV. Introducción

Wireshark, antes conocido como Ethereal, es un analizador de protocolos utilizado para realizar análisis y solucionar problemas en redes de comunicaciones, para desarrollo de software y protocolos, y como una herramienta didáctica para educación. Cuenta con todas las características estándar de un analizador de protocolos.

La funcionalidad que provee es similar a la de tcpdump, pero añade una interfaz gráfica y muchas opciones de organización y filtrado de información. Así, permite ver todo el tráfico que pasa a través de una red (usualmente una red Ethernet,



aunque es compatible con algunas otras) estableciendo la configuración en modo promiscuo. También incluye una versión basada en texto llamada tshark.

Permite examinar datos de una red viva o de un archivo de captura salvado en disco. Se puede analizar la información capturada, a través de los detalles y sumarios por cada paquete. Wireshark incluye un completo lenguaje para filtrar lo que queremos ver y la habilidad de mostrar el flujo reconstruido de una sesión de TCP.

Wireshark es software libre, y se ejecuta sobre la mayoría de sistemas operativos Unix y compatibles, incluyendo Linux, Solaris, FreeBSD, NetBSD, OpenBSD, y Mac OS X, así como en Microsoft Windows.

V. Conocimientos previos

- Dispositivos de red
- Concepto general de direcciones IP
- Concepto de direcciones física - MAC

VI. Procedimiento

Actividad 1: Exploración del programa packet tracer

A fin de analizar los paquetes de red y los protocolos de estos, wireshark ofrece una interfaz gráfica con una serie de paneles y herramientas (Ver Figura. 4) que facilitan el análisis de paquetes. Entre estos paneles se tiene: el panel de lista de paquetes, detalle paquetes y panel de examinación de bytes.



UNIVERSIDAD NACIONAL DE INGENIERÍA
FACULTAD DE ELECTOTECNIA Y COMPUTACIÓN
Departamento de Sistemas Digitales y Telecomunicaciones
Managua, Nicaragua

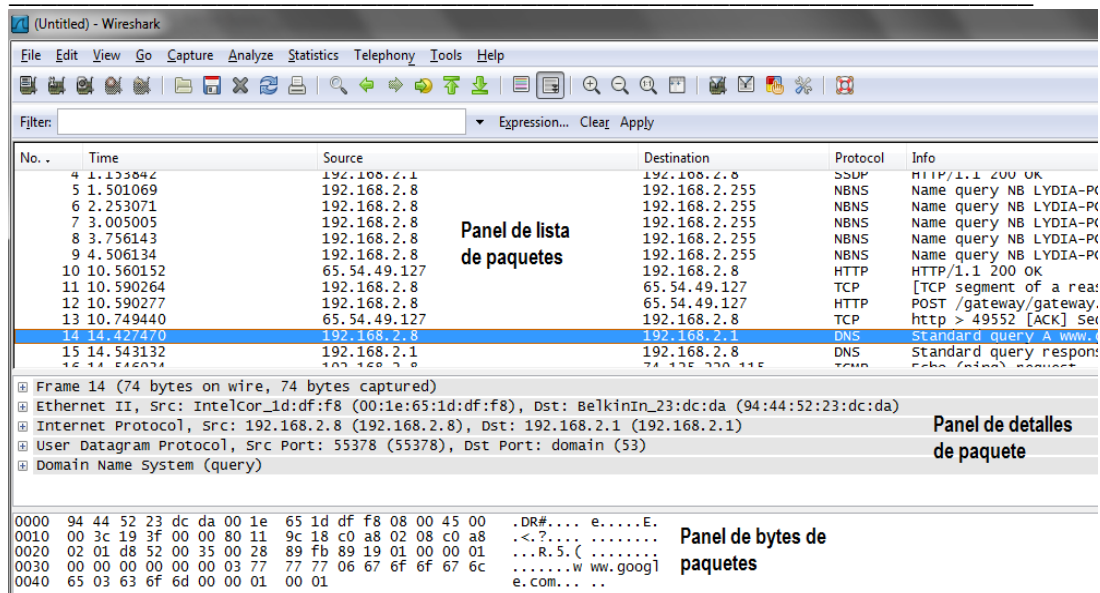


Figura. 4

Barra de herramientas de wireshark

La barra de herramientas de wireshark (Ver Figura. 5) posee un campo para el filtrado de paquetes utilizando expresión para indicar el paquete que se desea analizar.

La barra inferior permite el análisis de protocolo para redes inalámbricas

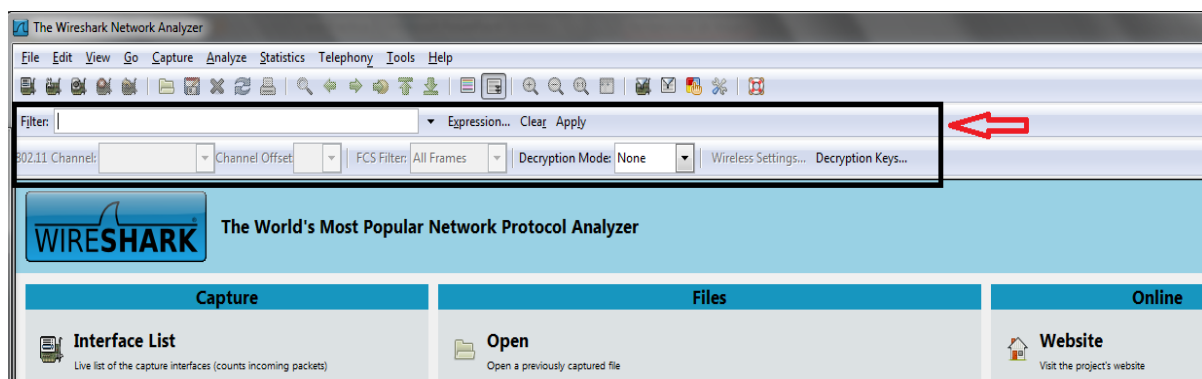


Figura. 5

Dentro de esta barra se encuentra la pestaña “expression...” se pueden observar el tipo de comandos utilizados para especificar el tipo de paquete que se desea filtrar de la captura total.

En la Figura. 6 se pueden observar algunos puntos resaltados como el área “relation” el cual se ocupa en el momento que se desean filtrar los paquetes para encontrar un paquete o tipo de paquete en específico.

El campo “Field name” (Ver Figura. 6) permite buscar las distintas abreviaciones para buscar los protocolos. Si no se ocupa el nombre correcto para buscar el protocolo la búsqueda no dará resultados positivos.

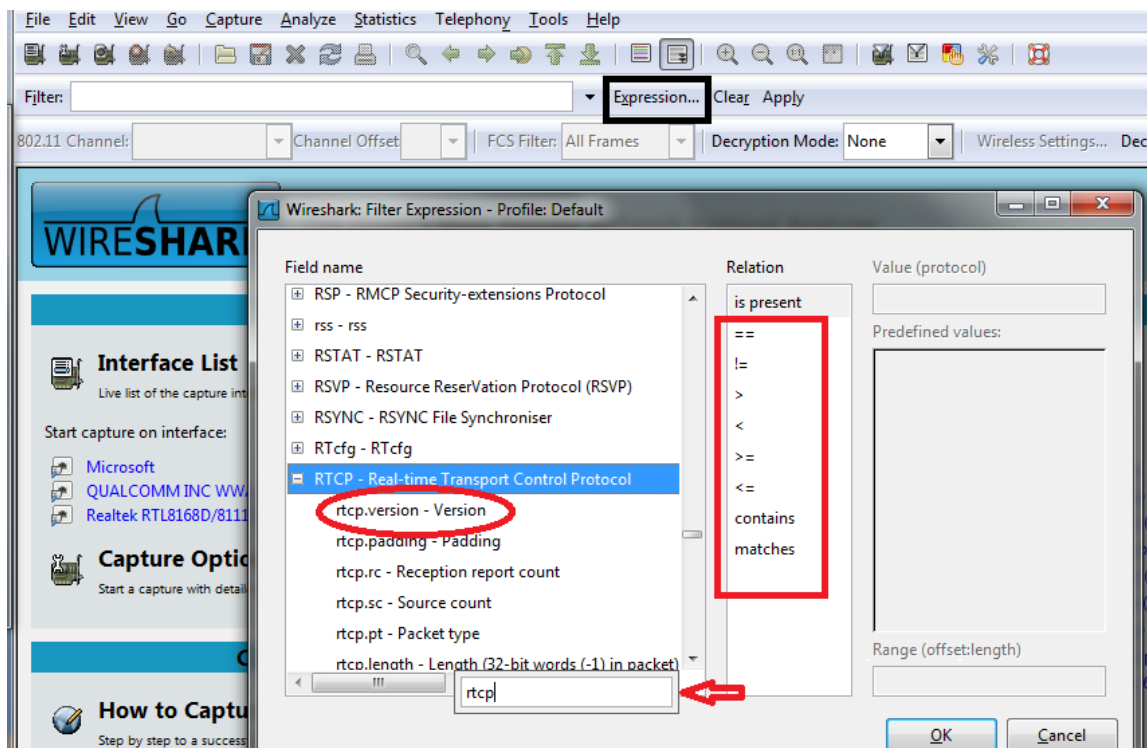


Figura. 6

En la pestaña de captura (Ver Figura. 7) se pueden configurar opciones como:

- La interfaz a utilizar.
- La habilitación de captura a paquetes promiscuos.
- El filtro de captura
- Resolución de nombres

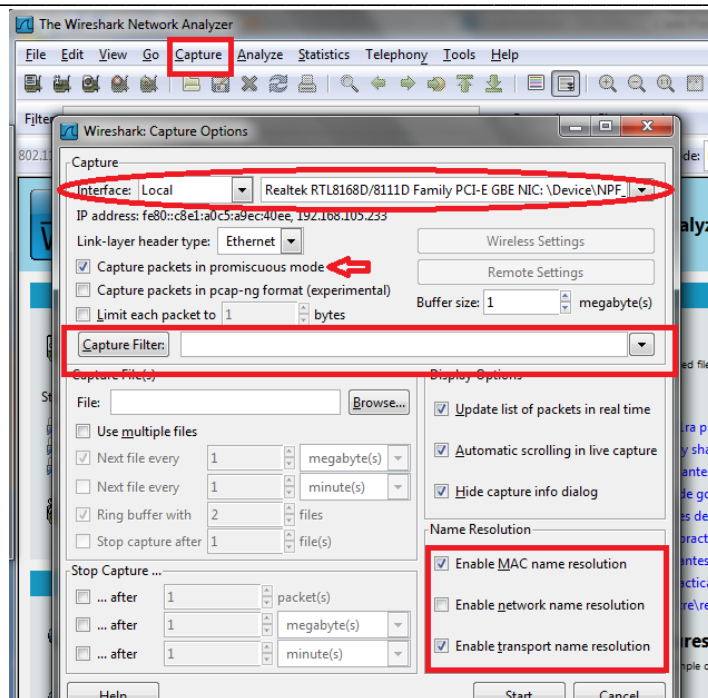


Figura. 7

La pestaña de análisis (Ver Figura. 8) contiene la opción de desplegar algunos comandos que se pueden ejecutar para realizar el filtrado de paquetes.

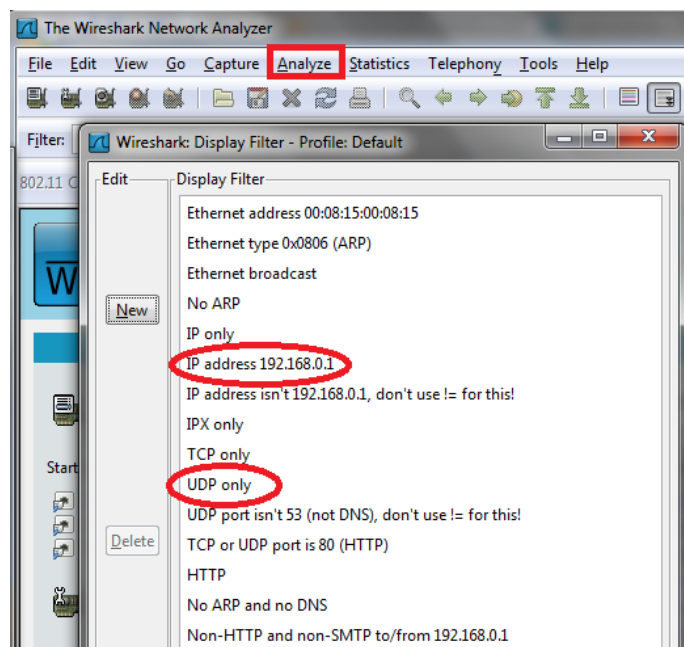


Figura. 8

Otra de las opciones es que Wireshark permite el seguimiento de sesiones TCP, UDP y SSL. En la pestaña *Analyze* se encuentran las opciones de seguir cadena (Ver Figura. 9).

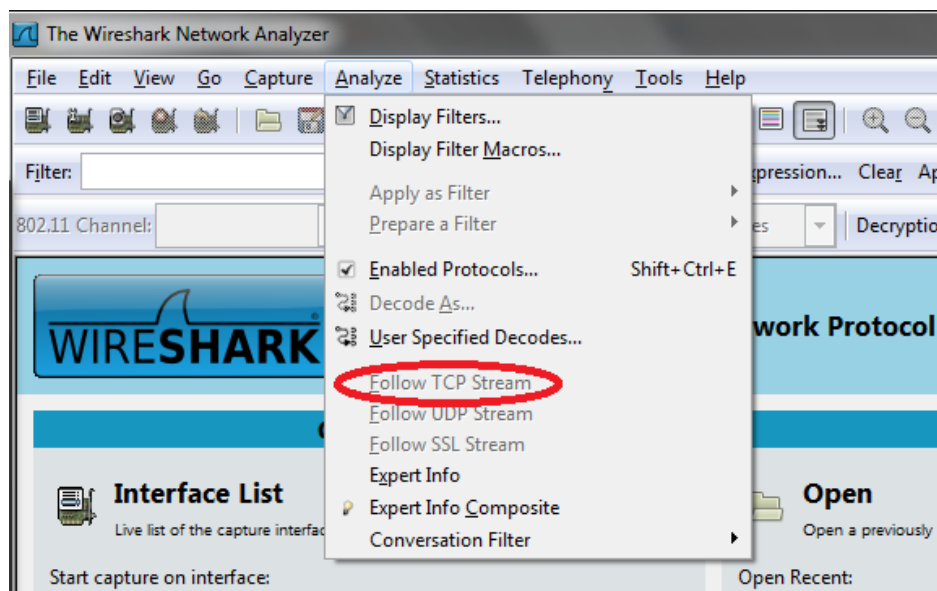


Figura. 9

Actividad 2: Captura de paquetes

Realice una captura de paquetes y utilice la función:

- Filtrado de paquetes por dirección IP
- Filtrado de paquetes por protocolo.

Para generar tráfico en la red puede utilizar el comando ping.

Actividad 3: Exploración de herramientas Wireshark

Wireshark ofrece pestaña llamada “Statistics”, esta pestaña facilita una serie de herramientas para el seguimiento y análisis visual de las conversaciones o sesiones establecidas entre los terminales.

La opción de estadísticas posee funciones que generan valores y gráficos a través del agrupamiento de paquetes acorde a (Ver Figura. 10):

- Direcciones IP
- Puntos finales
- Conversaciones entre hosts
- Gráficos de flujo de envío y recepción de protocolos.

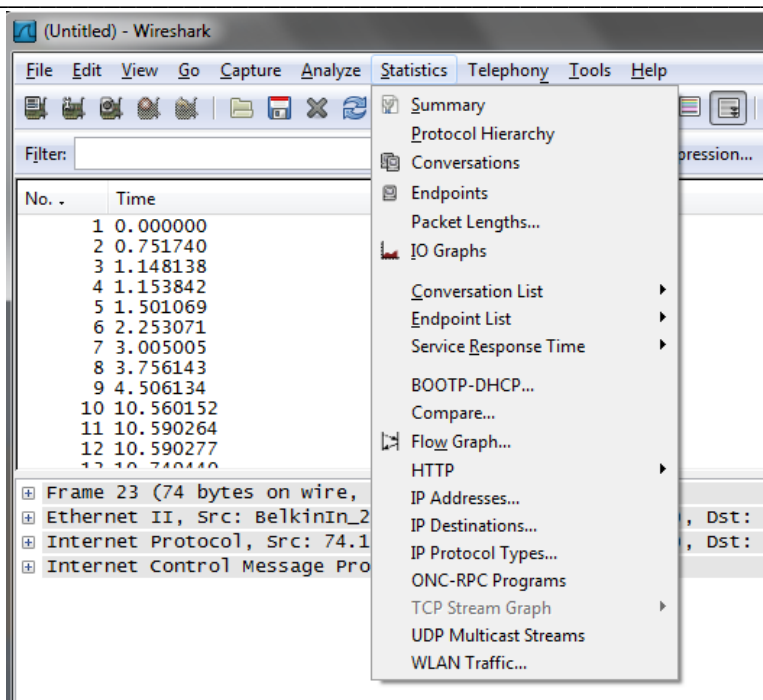


Figura. 10

Utilizando la opción “Conversation list” filtre la conversación de captura de los paquetes ICMP enviados con el comando ping de la sección anterior.

La pestaña de telefonía permite llevar a cabo el análisis de protocolos específicos de servicios para telefonía IP.

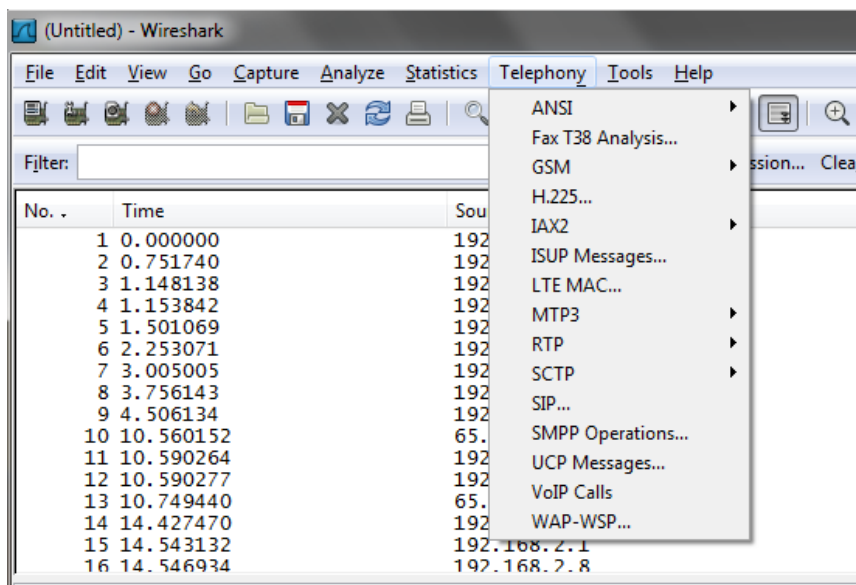


Figura. 11

Actividad 4: Filtrado de direcciones MAC.

1. Inicie la captura de paquetes utilizando el analizador de protocolos wireshark
2. Inicie el explorador de internet.
3. Agregue en 3 pestañas de la ventana principal 3 direcciones Web distintas.

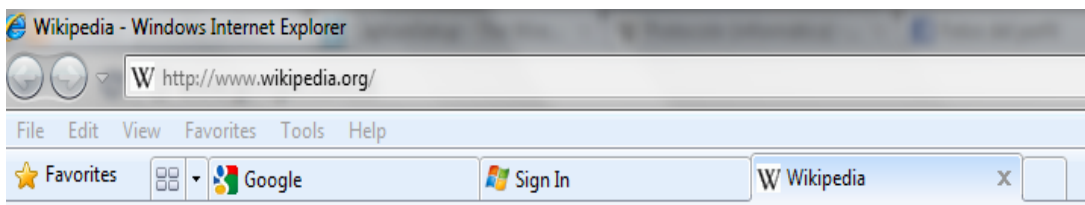


Figura. 12

4. Abra la ventana Ejecutar y escriba "cmd", luego procedemos a escribir arp – a.
5. Lo que nos mostrara un resultado similar a la figura.

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Owner>arp -a

Interface: 192.168.2.8 --- 0xb
Internet Address      Physical Address      Type
192.168.2.1           94-44-52-23-dc-da    dynamic
192.168.2.255         ff-ff-ff-ff-ff-ff    static
224.0.0.2             01-00-5e-00-00-02    static
224.0.0.252           01-00-5e-00-00-fc    static
239.255.255.250       01-00-5e-7f-ff-fa    static
255.255.255.255       ff-ff-ff-ff-ff-ff    static

C:\Users\Owner>ping 192.168.2.1
```

Figura. 13

6. De esta lista tomaremos una dirección que pertenezca a un ordenador en la red local y utilizaremos el comando ping seguida de la dirección ip que corresponda a este.
7. Identifique las conversaciones que fueron establecidas a las páginas web y PC del laboratorio
8. Complete el siguiente cuadro.



Pagina Web	Dir MAC Origen	Dir MAC Destino
www.google.com		
www.hotmail.com		
www.Wikipedia.com		
Ping 192.168.2.1		

VII. Preguntas de control

8. ¿Qué es wireshark?
9. ¿Cuáles son las ventajas de wireshark sobre otros analizadores de protocolo?
10. ¿Para que funciona el comando ping?
11. ¿Cuáles son algunas de las facilidades de wireshark?
12. ¿Permite wireshark el análisis de protocolos telefónicos?



Laboratorio No. 3: Ejercicios introductorios a Redes de Datos

Curso	Capacitación en telefonía IP		
Modulo	Redes de Datos	Grupo	
Tipo Practica	<input type="checkbox"/> Laboratorio <input type="checkbox"/> Simulación		
Unidad Temática			
No Alumnos por practica	1	Fecha	
Nombre del Profesor			
Nombre(s) del Alumno(s)			
Tiempo estimado	75 minutos	Vo. Bo. Del Docente	
Comentarios			

Objetivos de la práctica de laboratorio

I. Objetivo General

1. Adquirir conocimiento y habilidades en el diseño de redes IP

II. Objetivos específicos

1. Realizar conversiones binarias a hexadecimales y viceversa
2. Comprender las diferencias entre los tipos de máscaras por clase.
3. Verificar los resultados a través de simulaciones.

III. Medios a utilizar

- Equipo de cómputo
- Programa simulador de redes Packet tracer
- Calculadora

IV. Introducción

El laboratorio presenta una serie de ejercicios sobre operaciones básicas y necesarias para el diseño de redes IP. La conversión de octetos binarios a valores decimales enteros es importante para establecer los valores en la máscara de redes de cada host y asignación de direcciones IP. El desarrollo correcto de este procedimiento evita los conflictos entre ordenadores por el uso repetido de direcciones.



La máscara de una red o dirección IP es una combinación de 4 octetos de números binarios. Permite diferenciar la parte de dirección de red de la parte de dirección de host en la dirección IP del dispositivo. A través de esta distinción, un router determinar a qué red enviar los datos recibidos. Por ejemplo, si el router tiene la IP 192.168.1.1. y mascara de red 255.255.255.0, quiere decir que todo dato que se envíe con la dirección IP 192.168.1.1 deberá ir a la red local en la que se conecta. De lo contrario será enviado a Internet.

El siguiente cuadro demuestra el cómo se le es asignada una máscara de red a una subred en dependencia del valor del primero octeto que esta tenga.

Clase	Bits	IP Subred inicial	IP Broadcast	Mascara de decimal
A	0	0.0.0.0	127.255.255.255	255.0.0.0
B	10	128.0.0.0	191.255.255.255	255.255.0.0
C	110	192.0.0.0	223.255.255.255	255.255.255.0
D	1110	224.0.0.0	239.255.255.255	
E	1111	240.0.0.0	255.255.255.254	

V. Conocimientos previos

- Conceptos básico sobre números binarios
- Manejo de programa packet tracer
- Clasificación de máscaras de red según clase

VI. Procedimiento

Actividad 1. Complete el siguiente cuadro con las conversiones correspondientes.



$\times 10^6$	$\times 10^5$	$\times 10^4$	$\times 10^4$	$\times 10^3$	$\times 10^2$	$\times 10^1$	$\times 10^0$	Valor en decimal
1	0	0	1	0	0	1	0	
0	1	1	1	0	1	1	1	
1	1	1	1	1	1	1	1	
1	1	0	0	0	1	0	1	
1	1	1	1	0	1	1	1	
0	0	0	1	0	0	1	1	
1	0	0	0	0	0	0	1	
0	0	1	1	0	0	0	1	
0	1	1	1	1	0	0	0	
1	1	1	1	0	0	0	0	
0	0	1	1	1	0	1	1	
0	0	0	0	0	1	1	1	
0	0	0	1	1	0	1	1	
1	0	1	0	1	0	1	0	
0	1	1	0	1	1	1	1	
1	1	1	1	1	0	0	0	
0	0	1	0	0	0	0	0	
0	1	0	1	0	1	0	1	
0	0	1	1	1	1	1	0	
0	0	0	0	0	0	1	1	
1	1	0	0	0	0	0	0	



Actividad 2. Identifique la clase de la máscara que se debe asignar a cada una de las siguientes direcciones IP.

Dirección IP	Clase de la máscara
10.250.1.1	
150.10.15.0	
192.14.2.0	
148.17.9.1	
193.42.1.1	
193.42.1.1	
126.8.156.0	
220.200.23.1	
230.230.45.58	
177.100.18.4	
119.18.45.0	
249.240.80.78	
199.155.77.56	
117.89.56.45	
215.45.45.0	
199.200.15.0	
95.0.21.90	
33.0.0.0	
158.98.80.0	
219.21.56.0	

Actividad 3. Simule el siguiente escenario utilizando el software Packet tracer

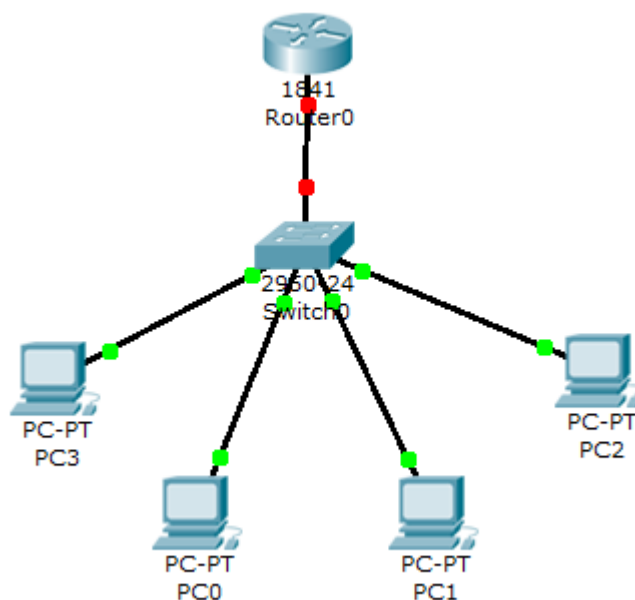


Figura 8 Escenario de una red LAN

- La red presentada tiene una dirección IP de red 192.168.2.0.
- Defina la dirección de máscara por clase correspondiente a esa dirección.
- Asigne las direcciones IP a cada máquina
- Asigne las máscaras de red correspondiente.
- Haga una Tabla donde se muestren las direcciones y máscaras de red de las PCs y del router.

1. Configuración de Router.

- Conecte un cable de consola desde una PC al router.
- De click sobre la PC donde conecto el cable de consola, seleccione la pestaña Desktop y luego la opción Terminal para acceder al Router.

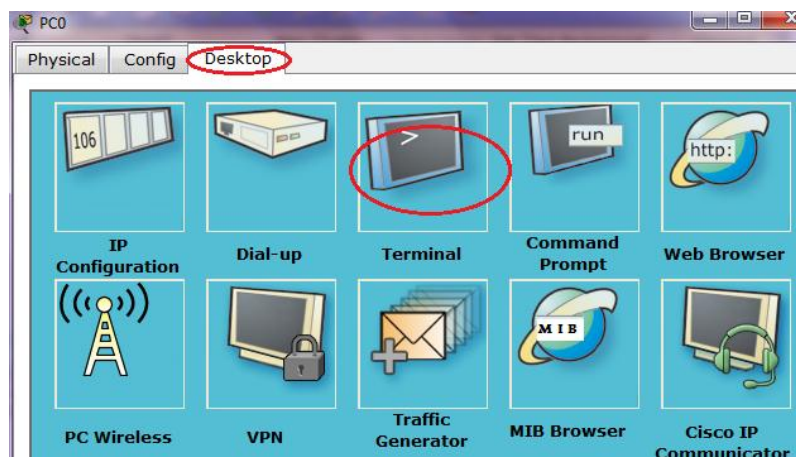


Figura 9 Ilustración de cómo se accede al terminal de la pc

- Luego presione ok al mensaje de Configuración de Terminal.
- Proceda a introducir los comandos para configuración del router:

```
Router>enable
```

```
Router#configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
Router(config)#hostname Router1
```

```
Router1(config)#interface fa 0/0
```

```
Router1(config-if)#ip address 192.168.2.1 255.255.255.0
```

```
Router1(config-if)#no shutdown
```

```
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0,  
changed state to up
```

```
Router1(config-if)#exit
```

```
Router1(config)#exit
```

```
Router1#
```

2. Asigne dirección IP, la máscara de red y gateway correspondiente a cada computador:



- De click sobre la PC que desea configurar.
- Elija la pestaña Desktop y la opción IP configuration.
- En la ventana que se le abrirá escriba los parámetros de red del computador.

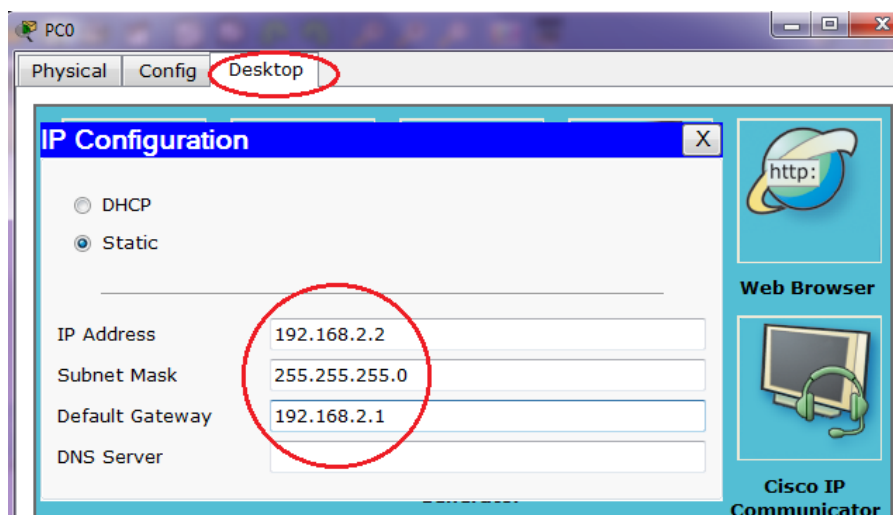


Figura 10 Configuración dirección IP de PC

2. Una vez realizada la etapa anterior verifique el funcionamiento correcto de la red, enviando paquete ICMP entre las computadoras. Para ello deberá dar doble-click en algún ordenador y luego buscar la pestaña Desktop. Luego inicie la ventana de comand prompt y escriba el siguiente comando:

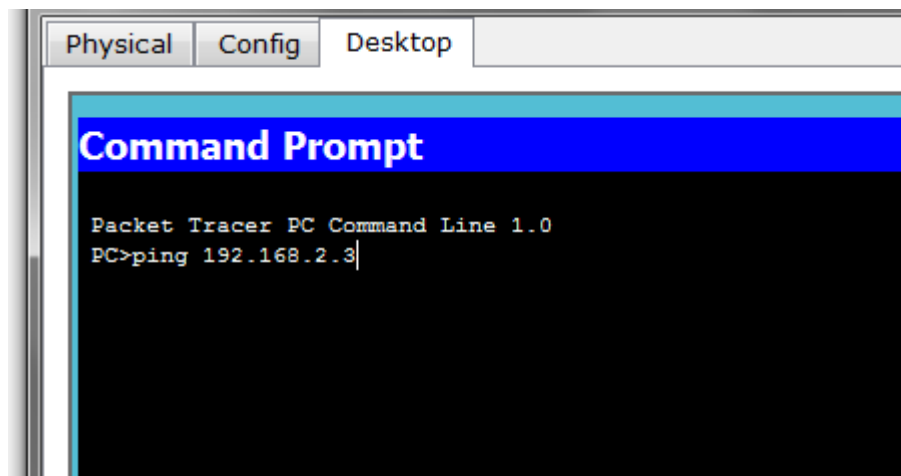


Figura 11 Comand Prompt



Este comando permitirá enviar 4 mensajes ICMP de 32 bits al ordenador que tenga la dirección en pantalla. Realizar este procedimiento hacia el router probando su buen funcionamiento.

VII. Preguntas de control

1. ¿Cuál es la función principal de la máscara de red?
2. ¿Cuál es el tiempo que tarda en enviar o recibirse un mensaje ICMP?
3. ¿Por qué los leds de las computadoras y switch iniciaron en anaranjados y luego cambiaron? ¿Qué sucede en ese momento?
4. ¿Hasta qué momento cambiaron los leds del router de rojo a verde? Y ¿Por qué?

VIII. Trabajo previo

Investigar ¿qué es ICMP? y ¿cómo funciona en los equipos de red?
Leer sobre el proceso de conversión de números binarios a decimal.



Laboratorio No. 4: Direccionamiento de tramas

Curso	Capacitación en telefonía IP		
Modulo	Redes de Datos	Grupo	
Tipo Practica	<input type="checkbox"/> Laboratorio	<input type="checkbox"/> Simulación	
Unidad Temática			
No Alumnos por practica	1	Fecha	
Nombre del Profesor			
Nombre(s) del Alumno(s)			
Tiempo estimado	75 minutos	Vo. Bo. Del Docente	
Comentarios			

Objetivos de la práctica de laboratorio

I. Objetivo General

1. Adquirir conocimiento sobre los distintos tipos de redes.

II. Objetivos específicos

1. Identificar los protocolos de redes LAN
2. Comprender el proceso de iniciación de equipos de red.
3. Verificar el proceso a través del modo simulación.

III. Medios a utilizar

- Equipo de cómputo
- Programa simulador de redes IP

IV. Introducción

El laboratorio presenta una serie de ejercicios y escenarios para facilitar la comprensión del funcionamiento del equipo de la red LAN y los protocolos con lo que estos operan. Los protocolos como ARP, ICMP, STP y DTP serán los protocolos en los cuales nos enfocaremos en esta práctica.



Se proporcionan las herramientas y escenario necesarios para el entendimiento del como los paquetes son enviados entre las terminales sin el uso del protocolo IP. A través de esta práctica los estudiantes podrán valorar las funciones que poseen los protocolos de iniciación.

El direccionamiento de tramas es estudiado a través del estudio de sus protocolos. Las direcciones MAC tiene una gran importancia pues identifica a cada dispositivo con un código único. Sin embargo con esta práctica el estudiante logra crear sus propios criterios sobre las ventajas y desventajas que involucra el uso de direcciones MAC como sistema de direccionamiento.

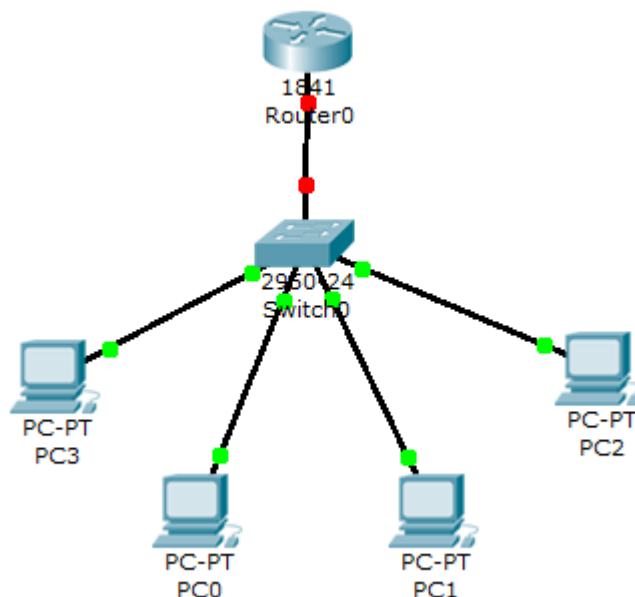
V. Conocimientos previos

- Concepto y funcionamiento del protocolo ICMP y ARP.
- Manejo de programa packet tracer

VI. Procedimiento

Actividad 1. Captura de protocolos

- Inicie el programa Packet tracer, luego seleccione la pestaña simulación y proceda a construir el siguiente esquema.



1. Configure las PC con las direcciones IP 192.168.2.2 hasta 192.168.2.5 junto con la dirección de puerta de enlace predeterminado 192.168.2.1 y la máscara de red 255.255.255.0. Luego configure la dirección del router con 192.168.2.1.
2. Configure el puerto Fastethernet Fa 0/0 con la dirección IP 192.168.2.1 con los siguientes comandos:
 - Conecte un cable de consola desde una PC al router.
 - De click sobre la PC donde conecto el cable de consola, seleccione la pestaña Desktop y luego la opción Terminal para acceder al Router.

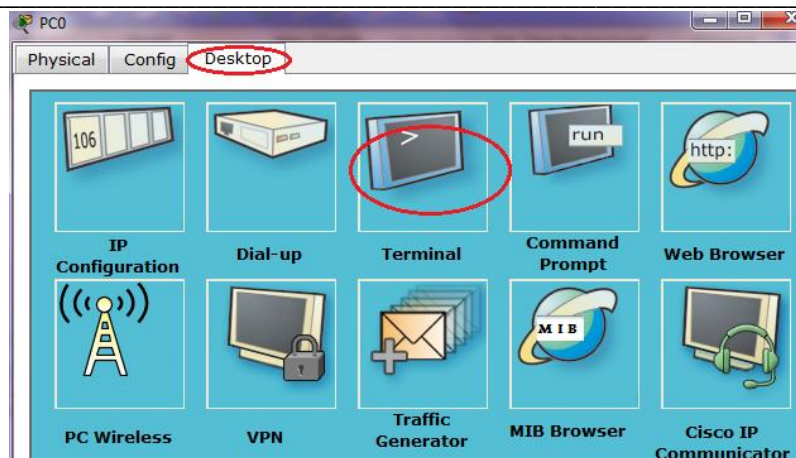


Figura 12 Ilustración de cómo se accede al terminal de la pc

- Luego presione ok al mensaje de Configuración de Terminal.
- Proceda a introducir los comandos para configuración del router:

Router>enable

Router#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#hostname Router1

Router1(config)#interface fa 0/0

Router1(config-if)#ip address 192.168.2.1 255.255.255.0

Router1(config-if)#no shutdown

Router1(config-if)#exit

Router1(config)#exit

Router1#

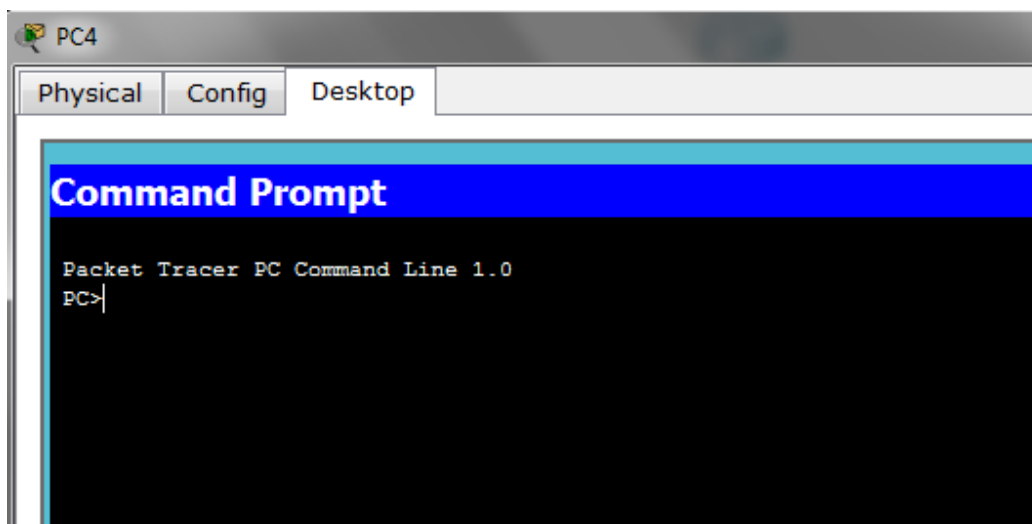
3. A continuación utilizando el modo de simulación de click en la opción Capture/Forward observe los protocolos que son utilizados y lo que sucede a medida que los paquetes son enviados.
4. Proceda a enviar un paquete desde una PC a otra y observe el proceso.
¿Qué diferencias encontró entre ambas pruebas?



Actividad 2. Definir tablas de ARP

Con el mismo esquema de red procederemos a explorar la creación, actualización, modificación y eliminación de direcciones físicas y lógicas de las tablas Mac existentes en los ordenadores.

1. De doble click sobre una de las PC. Luego busque la pestaña Desktop y seleccione Command Prompt. Debe obtener la siguiente ventana.



2. Una vez abierta, procedemos a escribir el comando `arp -a`. Esto nos mostrara las direcciones lógicas que la computadora ha almacenado en su tabla ARP asociando cada dir Ip a una dirección MAC. Observe cuales son los valores que se encuentran en la tabla.

3. A continuación envíe un paquete desde la PC en donde ha revisado la tabla ARP hacia otra PC, siga el transcurso del paquete hasta que este finalice. Vuelva a revisar la tabla ARP.

¿Ha tenido algún cambio la tabla de direcciones?

4. Realice el mismo proceso entre todas las computadoras y observe como cambian las tablas de direcciones MAC.

5. Envíe un paquete nuevamente y observe los paquetes que son enviados entre las PC.

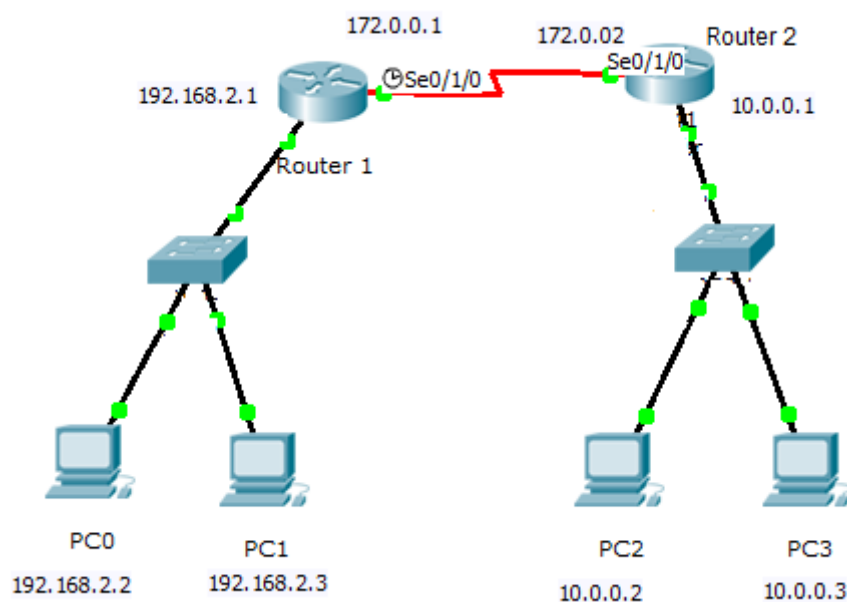
¿Hay algún cambio en ellos?

6. Utilice el comando **ARP /?** para revisar que otros comandos están asociados a esta expresión. Algunos de estos comandos permiten editar o modificar la lista de direcciones existentes o hasta incluso borrarla por completo.

7. En la PC en que se encuentra inicie la ventana ejecutar y luego escriba cmd. En esta parte escriba la expresión ARP /? . Haga una tabla con todas las opciones de ARP y sus respectivas funciones.

Actividad 3. Direcciones MAC fuera de la red LAN

Se construirá el escenario que se muestra en la figura siguiente:



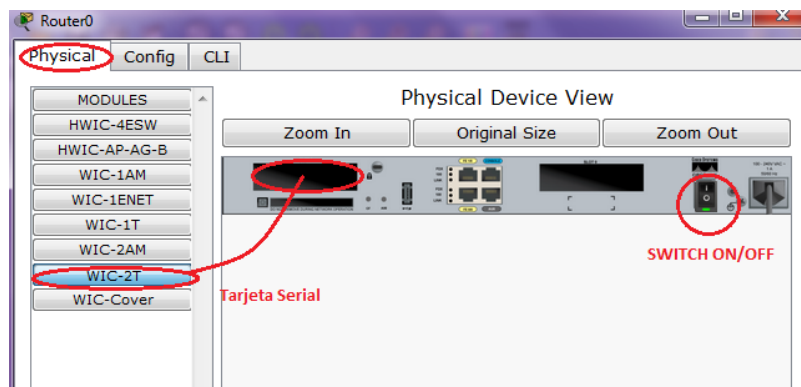
1. Según la gráfica anterior complete la tabla de las direcciones IP y máscara de red por clase de los dispositivos de la red.



Dispositivo	Interfaz	Dirección IP	Mascara de Red por clase
Router 1	Fastethernet		
	Serial		
Router 2	Fastethernet		
	Serial		
PC0	Fastethernet		
PC1	Fastethernet		
PC2	Fastethernet		
PC3	Fastethernet		

2. Para realizar la conexión WAN se debe de instalar la interface serial dentro de los dos router de la siguiente manera:

- De click sobre el router y seleccione la pestaña Physical.
- Apague el router dando click sobre el switch on/off que aparece en la parte derecha de la imagen del Router.
- Arrastre la tarjeta serial WIC-2T sobre una ranura vacía del router.



- Encienda el router.
3. Realice todas las conexiones del escenario.
4. Configure las interfaces Fastethernet Fa 0/0 y serial s 0/0/0 de los router con sus respectivas direcciones IP y máscaras de red.
- Conecte una de las PC y el router con un cable de consola.
 - Entre al terminal de la PC que conecto e introduzca los comandos de configuración:
 - Con sus respectivas direcciones IP



```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R1
R1(config)#interface fa 0/0
R1(config-if)#ip address 192.168.2.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface s 0/1/0
R1(config-if)#ip address 172.0.0.1 255.255.0.0
R1(config-if)#clock rate 64000
R1(config-if)#no shutdown
R1(config-if)#
R1#
```

- Luego se configura el router 2 de la misma manera pero con las direcciones IP correspondientes y sin el clock rate ya que solo uno de los dos terminales debe de poseerlo.
5. Proceda a asignar las direcciones IP a las PCs y su direcciones Gateway correspondientes.
 6. Revise las tablas ARP de cada uno de los ordenadores. Una vez realizado esto envíe paquetes de datos entre las PC repitiendo el proceso realizado en la actividad anterior.

Nuevamente revise las tablas ARP.

¿Nota alguna diferencia?

¿Qué sucede con las direcciones MAC que provienen de PCs de otras redes?
Explique brevemente.



VII. Preguntas de control

5. ¿Qué tipo de paquetes de datos son intercambiados al iniciar una red?
6. ¿Qué es una tabla ARP?
7. ¿En qué área de las redes de datos operan las direcciones MAC?
8. ¿Cuál es la importancia de las direcciones MAC?

VIII. Trabajo previo

Investigar sobre los protocolos STP, ARP, ICMP y DTP.



Laboratorio No. 5: Protocolos HDLC y PPP.

Curso	Capacitación en telefonía IP		
Modulo	Redes de Datos	Grupo	
Tipo Practica	<input type="checkbox"/> Laboratorio <input type="checkbox"/> Simulación		
Unidad Temática			
No Alumnos por practica	1	Fecha	
Nombre del Profesor			
Nombre(s) del Alumno(s)			
Tiempo estimado	60 minutos	Vo. Bo. Del Docente	
Comentarios			

Objetivos de la práctica de laboratorio

I. Objetivo General

1. Comprender como los protocolos de encapsulamiento WAN afectan los enlaces seriales.

II. Objetivos específicos

1. Mostrar las características de un enlace HDLC.
2. Convertir enlaces que usan HDLC a protocolo PPP.
3. Configurar los modos de autenticación del protocolo PPP.

III. Medios a utilizar

- Equipo de computo
- Programa simulador de redes IP Packet Tracer

IV. Introducción

El laboratorio a desarrollar se enfoca en el estudio de protocolo de enlace en áreas amplias, específicamente los protocolos HDLC y PPP. Estos protocolos se ubican en la capa 2 de enlace de datos del modelo OSI.

HDLC es un protocolo derivado de SDLC y fue desarrollado por la ISO, pero ha sido implementado de diferentes formas por cada fabricante. HDLC especifica un formato de encapsulación de trama para enlaces de datos sincrónicos, orientado a



la conexión. Se utiliza frecuentemente para trabajar sobre líneas punto a punto dedicadas.

PPP provee servicios para conexiones de router a router o terminal a terminal, en circuitos síncronos y asíncronos usando interfaces seriales. Es comúnmente usado por las PCs para conectarse a proveedor de servicios de internet (ISP) a través de una línea telefonica o como un método de encapsulamiento WAN entre LANs.

PPP es considerado parte de la suite de protocolo TCP/IP y soporta una variedad de protocolos LANs como IP o IPX y varios métodos de autenticación de seguridad como PAP y CHAP. En realidad, PPP es usado como una variación de HDLC para encapsulamiento de paquetes.

Casi todas las conexiones WAN usadas para Internet son seriales. Los router tienen puertos seriales síncronos para este tipo de conexiones. Estos puertos no son iguales a los asíncronos que poseen las PCs y son capaces de transmitir a velocidad mucho más altas. La mayoría de los router tienen por lo menos un puerto serial síncronos y 2 puertos asíncronos.

Las velocidades para enlaces WAN digitales seriales pueden variar de entre 56Kbps hasta circuitos de T1 lo que representa 1.5 Mbps o un T3 de 45 Mbps, aproximadamente.

En los equipos CISCO, los enlaces WAN por defecto utilizan el protocolo HDLC. PPP es más estandarizado en cuanto a proveer mejor seguridad y soportar conexiones llamantes. Sin embargo, el protocolo PPP debe ser configurado en ambos extremos para su bien funcionamiento.

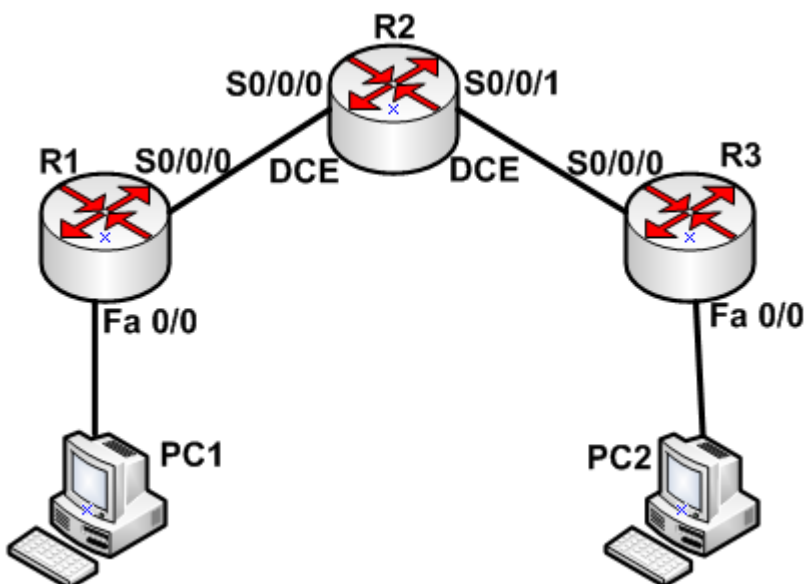


V. Conocimientos previos

- Protocolos HDLC y PPP
- Protocolo de autenticación PAP y CHAP
- Programación básica de interfaces seriales
- Asignación de direcciones IP

VI. Procedimiento

Actividad 1. Configuración del escenario



Dispositivo	Puerto	Dirección IP	Mascara de red	Gateway
PC1	Ethernet	10.0.0.1	Clase C	10.0.0.2
R1	Fa 0/0	10.0.0.2	Clase C	-----
R1	S 0/0/0	10.0.1.1	Clase C	-----
R2	S 0/0/0	10.0.1.2	Clase C	-----
R2	S 0/0/1	10.0.2.1	Clase C	-----
R3	S 0/0/0	10.0.2.2	Clase C	-----
R3	Fa 0/0	10.0.3.1	Clase C	-----
PC2	Ethernet	10.0.3.2	Clase C	10.0.3.1



Paso 1. Interconecte los dispositivos según muestra la figura anterior.

Recuerde que los enlaces entre los router R1, R2 y R3 son seriales. Y al momento de conectarlos debe utilizar el cable DCE iniciado en R2 para que se reconozca que este será el DCE.

En el caso de las interfaces seriales deberá agregar los módulos seriales antes de conectarlos.

Paso 2. Proceda a asignar las direcciones IP a las terminales de los dispositivos, según se muestran en la tabla de referencia.

Paso 3. Configure las terminales DCE con un clock rate de 64000.

Paso 4. Una vez configurados los router utilice el siguiente comando en el router R2 y responda:

Show interface serial 0/0/1

¿Para qué sirve este comando?

¿Cuál es el estado de la interfaz y protocolo de línea?

¿Cuál es la unidad de transmisión máxima (MTU)?

¿Cuál es el ancho de banda establecido?



¿Cuál es el protocolo de encapsulamiento establecido por defecto?

Actividad 2: Remover el ancho de banda establecido por defecto

Paso 1: Utilice los siguientes comandos en el router R2.

```
R2# config t
R2(config)# int S0/0/1
R2 (config-if)# no bandwidth
```

Paso 2: Utilice nuevamente el comando sh int s 0/0/1 y responda:

¿Cuál es el valor del ancho de banda?

Paso 3: Cambie el ancho de banda a 56Kbits utilizando la siguiente serie de comandos:

```
R2# config t
R2(config)# int s 0/0/1
R2(config-if)# bandwidth 56
```

Paso 4: Verifique el cambio de ancho de banda en la interfaz s0/0/1, usando el comando sh int s 0/0/1 en R2.

¿Hubo algún cambio?



Actividad 2. Verificación de configuración en R2

Paso1. Utilice el comando `sh running – config` en el router R2 y responda:

¿Cuál es la interfaz serial usada en el enlace WAN?

¿Cuál es la dirección IP que se muestra para la interfaz serial S0/0/1?

¿Cuál es la máscara de red de la interfaz?

Según los resultados del comando “`sh controller s 0/0/1`”, ¿Qué tipo de conexión es la interfaz S0/0/1 DCE o DTE?

Actividad 3: Cambio de protocolo de enlace HDLC a PPP.

Paso 1: Entre a la interfaz de línea de comando del router R2.

Paso 2: Utilice la siguiente línea de comando



```
R2# sh interface serial 0/0/1
R2# config t
R2(config)# interface serial 0/0/1
R2(config-if)# encapsulation PPP
```

Paso 3: Realice el mismo proceso para la interfaz S 0/0/0 del router R2

¿Existe comunicación entre los terminales? ¿Por qué?

Paso 4: Configure las interfaces S 0/0/0 de los router R1 y R3 con para que utilicen el encapsulamiento PPP, como se mostró en el paso 2.

¿Existe comunicación entre los terminales?

Actividad 4: Autenticación CHAP

Paso 1: Seleccionamos el router R2 e iniciamos el CLI (interfaz de línea de comandos).

Paso 2: Es necesario establecer un usuario y password.

Para ello utilizaremos las siguientes líneas de comandos:

```
R3#config t
```



R3(config)# username "Carlos" password "123"

Este comando permite crear un usuario y password de autenticación para un dispositivo remoto que solicite una conexión con el router. Ambos parámetros son sensibles a mayúsculas y minúsculas.

Paso 2: Configuramos la encapsulación a utilizar en la interfaz S 0/0/1, con la secuencia de comandos:

R3# configure terminal

R3(config)# interface serial 0/0/1

R3(config – if)# encapsulation ppp

R3(config – if) # ppp authentication CHAP

Paso 3. Para verificar que el proceso de autenticación ha sido establecido correctamente usamos:

R3# show interfaces s0/0/1

R3# show running –config

Paso 4. En caso que se desee llevar a cabo el monitoreo de la actividad PPP en el router o interfaz, se pueden ocupar los comandos:

R3# debug PPP negotiation

R3# debug PPP authentication

Paso 5. Trate de iniciar una session Telnet hacia R2 desde CMD en PC2. Para ello deberá utilizar el comando:

Telnet 10.0.2.1



Actividad 5: Autenticación por PAP

Paso 1: En este caso, primero estableceremos el nombre de usuario y password:

R3# config t

R3(config)# interface serial 0/0/0

R3(config-if)# encapsulation ppp

R3(config-if)# ppp authentication pap

Paso 2: Sin embargo a partir de Cisco IOS 11.1 se debe habilitar PAP en la interface del router que debe enviar la información de autenticación.

En este caso haremos la conexión desde PC1, por lo tanto haremos uso de la interface S 0/0/0 de R1.

R1# config t

R1(config)# interface serial 0/0/0

R1(config-if)# encapsulation ppp

R1(config-if)# ppp pap sent-username "Carlos" password "123"

Paso 3: Verifique que la conexión funciona estableciendo una sesión telnet como se mostró anteriormente.

VII. Preguntas de control

1. ¿Qué es HDLC?
2. ¿Qué es PPP?
3. ¿Cuáles son los modos de autenticación de PPP?
4. ¿Cuáles son las diferencias entre los modos de autenticación de PPP?



5. ¿Cuáles son las ventajas de PPP sobre HDLC?

VIII. Trabajo previo

- ✓ Investigar sobre el funcionamiento de protocolos HDLC y PPP.
- ✓ Proceso de autenticación PAP y CHAP.



Laboratorio No. 6: Protocolo de capa de enlace Frame-Relay.

Curso	Capacitación en telefonía IP		
Modulo	Redes de Datos		Grupo
Tipo Practica	<input type="checkbox"/> Laboratorio	<input type="checkbox"/> Simulación	
Unidad Temática			
No Alumnos por practica	1	Fecha	
Nombre del Profesor			
Nombre(s) del Alumno(s)			
Tiempo estimado	75 minutos	Vo. Bo. Del Docente	
Comentarios			

Objetivos de la práctica de laboratorio

I. Objetivo General

1. Comprender el proceso de configuración para establecer redes Frame – Relay.

II. Objetivos específicos

1. Realizar una configuración básica de switchs frame- relay
2. Establecer parámetros de identificación de enlace de datos.
3. Configurar los equipos router fronterizos para establecer la comunicación.

III. Medios a utilizar

- Equipo de computo
- Programa simulador de redes IP – Packet tracer
- Calculadora.

IV. Introducción

El laboratorio presente se enfoca hacia el estudio del protocolo de conmutación de paquetes Frame – Relay para conectar dispositivos usando redes de área amplia WAN. Frame Relay es un estándar de la industria ubicado en la capa de enlace de datos del modelo TCP/IP, permite manejar multiples circuitos virtuales usando encapsulamiento HDLC entre dispositivos conectados, por ejemplo routers.



Frame relay es más efectivo que X.25, el protocolo para el cual es considerado un reemplazo. Es considerablemente más utilizado en las tecnologías de comunicación de redes WAN.

FR utiliza longitudes variables para paquetes para transferencias más efectivas y flexibles. Estos paquetes luego son conmutados entre varios segmentos de red hasta que el destino es alcanzado. Técnicas de multiplicación estática controlan el acceso a las redes. La ventaja de este método es que brinda más flexibilidad y más eficiencia en el uso del ancho de banda entre los switches dentro de la nube (red frame relay de tráfico).

Frame relay es una manera de compartir líneas T1 y T3 existentes y que son provistas por un proveedor de servicio y potencialmente mejorando el uso de estas. Más compañías de teléfonos ahora proveen servicios Frame Relay para los clientes que quieren conexiones de entre 56 Kbps hasta velocidad de T -1.

Los dispositivos asociados a redes WAN Frame relay pueden ser clasificados en dos categorías: Equipos de dato terminal (DTE) y Equipos de datos terminación de circuito (DCE). Los DTE son típicamente ubicados en la frontera o borde de la red del cliente. Ejemplo de estos son las terminales, computadoras personales, routers y puentes. Los DCE son usualmente dispositivos de internet del ISP pero pueden ser adquiridos por los clientes también. El propósito del equipo DCE es proveer el reloj de sincronización y conmutar servicios en una red. Estos DCE son los dispositivos que transmiten los datos sobre la red WAN, en la mayoría de los casos estos conmutan paquetes Frame – Relay por si solos.

Frame relay provee conexiones orientadas a comunicación en la capa de enlace de datos. Esto significa que una comunicación definida existe entre cada par de dispositivos y que esas conexiones son asociadas a un identificador de conexión. Este servicio es implementado usando circuitos virtuales, los cuales son



conexiones lógicas creadas entre dos DTE a través de la red de conmutación de paquetes. Los circuitos virtuales proveen una comunicación bi-direccional de un DTE al otro y son identificados por un DLCI.

Un número de circuitos virtuales pueden ser multiplexados en un circuito físico única para transmitirle a través de la red. Esta capacidad puede reducir número de dispositivos necesario para implementar la red y complejidad requerida para conectar múltiples dispositivos DCE. Un circuito virtual puede pasar a través de cualquier número de dispositivos DCE intermediarios ubicados dentro de la red FR. Los circuitos virtuales de una red FR se pueden agrupar en dos categorías: circuitos virtuales conmutados (SVC) y circuitos virtuales permanentes (PVC). Los PVCs son las comunes.

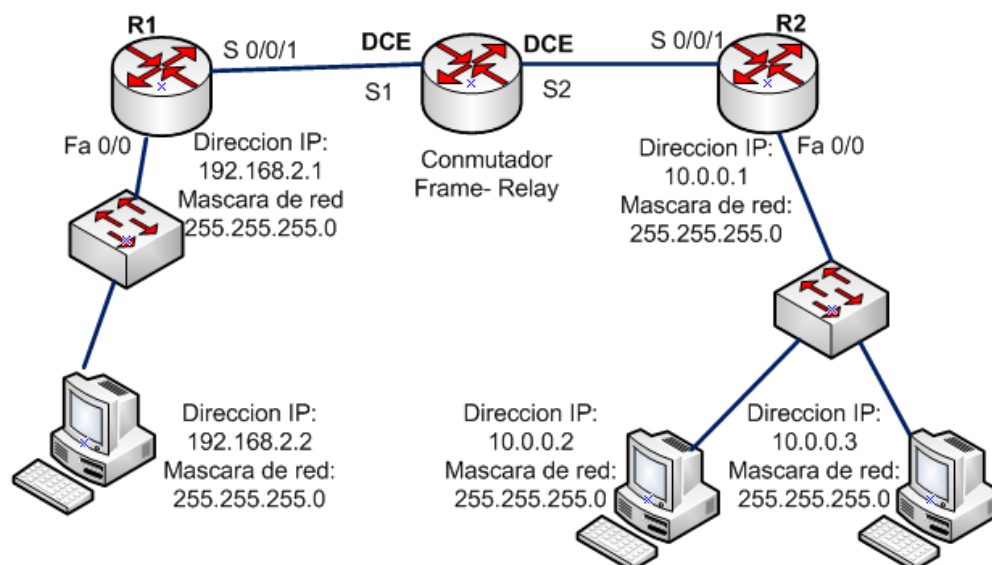
Este laboratorio será necesario configurar un router para configurar como switch Frame Relay y conectarlo a otros 2 routers a través de este Frame Relay switch para simular un área amplia entre 2 redes LAN.

V. Conocimientos previos

- Concepto Frame - Relay
- Identificador de enlace de datos
- Protocolo EIGRP.

VI. Procedimiento

Actividad 1. Configuración de direcciones IP.



Paso 1. Agregue las interfaces seriales a los router R1, R2 y R3 (este es un router que se configura como switch frame relay).

Proceda a configurar las direcciones IP de las computadoras e Interfaces Fa 0/0 de los router R1 y R2 de la topología mostrada en la figura anterior.

Utilice la tabla a continuación como referencia.

Dispositivo	Interfaz	Dirección IP	Mascara de red	Gateway
R1	Fa 0/0	192.168.2.1	Clase C	No aplica
R2	S 0/0/1	172.0.0.1	Clase C	No aplica
R2	Fa 0/0	10.0.0.1	Clase C	No aplica
R2	S 0/0/1	172.0.0.2	Clase C	No aplica
PC 1	Ethernet	192.168.2.2	Clase C	192.168.2.1
PC 2	Ethernet	10.0.0.2	Clase C	10.0.0.1
PC3	Ethernet	10.0.0.3	Clase C	10.0.0.1

Para configurar el router R1, utilice la siguiente secuencia de comandos.



Paso 2: Configuración Interfaz serial

```
Router1# config t
Router1 (config)# interface Serial 0/0/1
Router1 (config – if)# ip address “direccion IP” “maskara de red”
Router1 (config – if) # encapsulation frame – relay
Router1 (config – if)# no shutdown
```

Paso 3: Configuración Interfaz Ethernet Fa 0/0

```
Router1 (config)# interface Fa 0/0
Router1 (config – if) ip address “direccion IP” “maskara de red”
Rotuer1 (config – if)# no shutdown
```

Paso 4: Configuración de protocolo de enrutamiento EIGRP.

```
Router1 (config) # router eigrp 100
Router1 (config – router)# network “direcciones de red conectada”
Router1 (config – router)# network “direcciones de la otra red conectada”
```

Paso 5: Verifique que la configuración es correcta usando el comando:

```
Router1# sh run
```

Paso 6: Realice los pasos 1, 2, 3, 4 y 5 para el router R2.

Actividad 2: Configuración el router intermedio como conmutador Frame – Relay.

Paso 1: Entre a la pestaña CLI dentro de las opciones del router.

Paso 2: Habilitando conmutación Frame - Relay

Una vez ahí, proceda a ingresar la siguiente secuencia de comandos.

```
Router# config t
```



```
Router (config)# hostname switchFR
```

```
switchFR (config)# frame-relay switching
```

****Este último comando inicia el proceso de conmutación Frame – Relay****

Paso 3: Configuración de interfaces S 0/0/1

```
switchFR (config)# interface serial 0/0/1
```

*****Permite seleccionar la interfaz serial S1*****

```
switchFR (config – if)# no ip address
```

*****Especifica la direccion IP de la interfaz serial S1*****

```
switchFR (config – if)# encapsulation frame – relay
```

*** **Cambia el dipo de encapsulamiento de capa 2 de HDLC a Frame- Relay*****

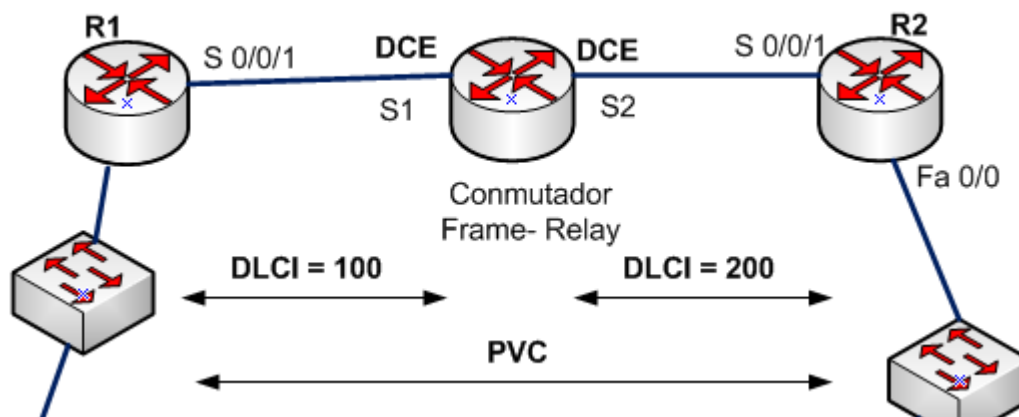
```
switchFR (config – if)# clock rate 56000
```

*** **Especifica el tasa del reloj de sincronización para el lado DCE de la interfaz*****

```
switchFR (config – if)# frame – relay intf – type dce
```

*** especifica la interfaz como un dispositivo DCE***

Para agregar las rutas que tomaran los paquetes que reciba la red Frame – Relay es necesario establecer los indicadores de comunicación y rutas de paquetes. La siguiente imagen muestra el cómo se ubica o interpretan en la red los DLCI y circuitos virtuales permanentes.



switchFR (config – if)# frame relay route “numero de ruta” interface serial “numero de interfaz serial” “identificador DLCI destino”

***Define la ruta de la trama de tal forma que los paquetes entrantes en la interfaz serial 0/0/1 con un identificador DLCI en específico deberá ir a las interfaz serial S 0/0/2.

Por ejemplo todo paquete que llegue a la interfaz serial S1 de la gráfica con el DLCI en 100, deberá ser enviado a de S2 con un DLCI de 200.

switchFR (config – if)# no shutdown

Paso 4: Configuración de la interfaz serial S2

Realice la misma secuencia de comando para la interfaz S2 ajustando la ruta que deben seguir los paquetes provenientes del router R2.

switchFR (config)# interface serial 0/0/1

switchFR (config – if)# no ip address

switchFR (config – if)# encapsulation frame – relay

switchFR (config – if)# clock rate 56000

switchFR (config – if)# frame – relay intf – type dce



switchFR (config – if)# frame relay route “*numero de ruta*” interface serial “*numero de interfaz serial*” “*identificador DLCI destino*”

switchFR (config – if)# no shutdown

Actividad 3. Verificación de configuración.

Paso 1: Use el comando “sh run” para visualizar la configuración actual del switch Frame – Relay.

Responda:

¿Qué información fue desplegada una vez que ejecuto el comando *sh run* en relación a la interfaz S 0/0/1?

¿Qué información fue desplegada una vez que ejecuto el comando *sh run* en relación a la interfaz S 0/0/2?

Paso 2. Ingrese al CLI de R1. Verifique la configuración del router R1 a través del estado del circuito virtual permanente (PVC). Para ello utilice el comando “show frame pvc”

Responda:

¿Cuál es el número de la conexión DLCI?



¿Cuál es el estado de la PVC?

¿Cuál es el número de la conexión DLCI?

Paso 5: En el switch frame relay. Utilice el comando “show frame pvc” y responda:

¿Cuáles son los números DLCI de las conexiones?

¿Cuál es el estado de los PVCs?

Paso 6: Verifique la conectividad de extremo a extremo de toda la red creada.

Para ello utilice el comando Ping. Realice este proceso en ambos sentidos de la red.

VII. Preguntas de control

1. ¿Qué es un PVC?
2. ¿Cuál es la función de los DLCI?
3. ¿Cuáles son las ventajas de Frame – Relay?
4. ¿Para qué sirve el comando *frame relay route*?
5. ¿Cuál es la diferencia entre DTE y DCE?

VIII. Trabajo previo

- ✓ Leer sobre PVC, DLCI e EIGRP.



Laboratorio No. 7: División de una red en subredes usando VLSM

Curso	Capacitación en telefonía IP		
Modulo	Redes de Datos	Grupo	
Tipo Practica	<input type="checkbox"/> Laboratorio <input type="checkbox"/> Simulación		
Unidad Temática			
No Alumnos por practica	1	Fecha	
Nombre del Profesor			
Nombre(s) del Alumno(s)			
Tiempo estimado	45 minutos	Vo. Bo. Del Docente	
Comentarios			

Objetivos de la práctica de laboratorio

I. Objetivo General

1. Adquirir conocimientos y habilidades en el diseño de redes IP a través del uso de VLSM.

II. Objetivos específicos

1. Realizar cálculos para la división de la red en subredes.
2. Configurar los dispositivos del simulador para su prueba.
3. Verificar que todos los escenarios funcionen correctamente.

III. Medios a utilizar

- Calculadora
- Equipo de computo
- Programa simulador de redes IP

IV. Introducción

Este laboratorio presenta una serie de ejercicios para aumentar las habilidades que se tienen para la división de una red en varias subredes. Es de gran importancia pues es muy frecuente el crear redes IP dentro de otras redes IP para lo cual es necesaria la variación de la máscara de subred.

El sistema de máscaras de red por clase tiene grandes desventajas pues el número de host está definido para cada mascara y no puede variarse. Si se desea limitar el número de usuarios en una red, este no puede ser a la medida deseada.



El diseñador debería ajustar el número de ordenadores o host a la cantidad de direcciones disponibles.

En cambio al utilizar VSLM se tiene una mayor flexibilidad en cuanto al número de usuarios deseados por subred brindando así un mayor orden que facilita la administración de esta.

V. Conocimientos previos

- Protocolo IP.
- Máscaras de red
- Conversiones de binario a decimal y viceversa.

VI. Procedimiento

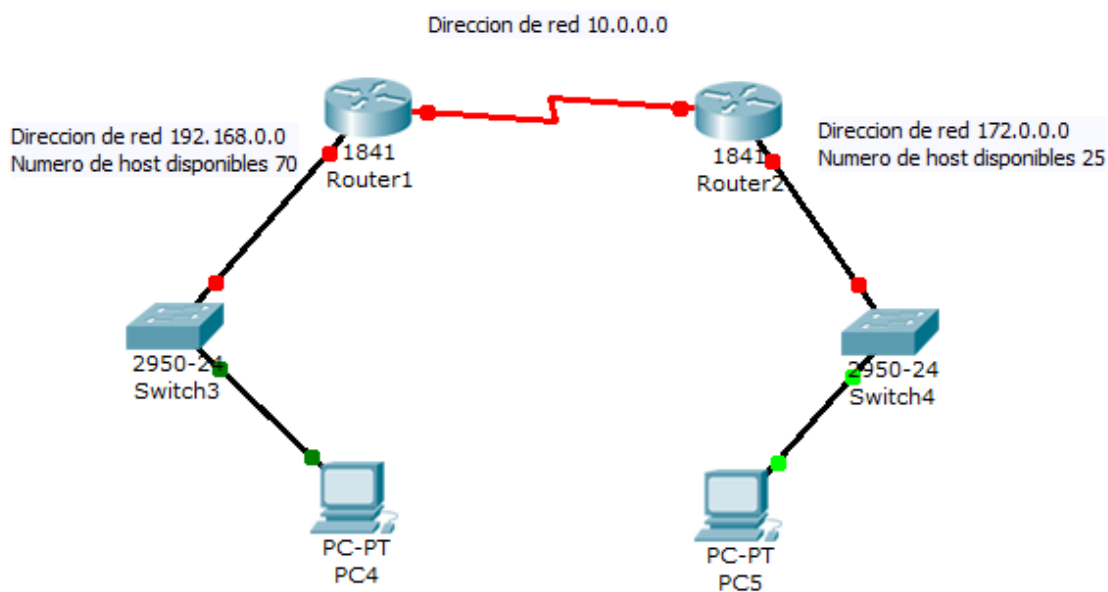
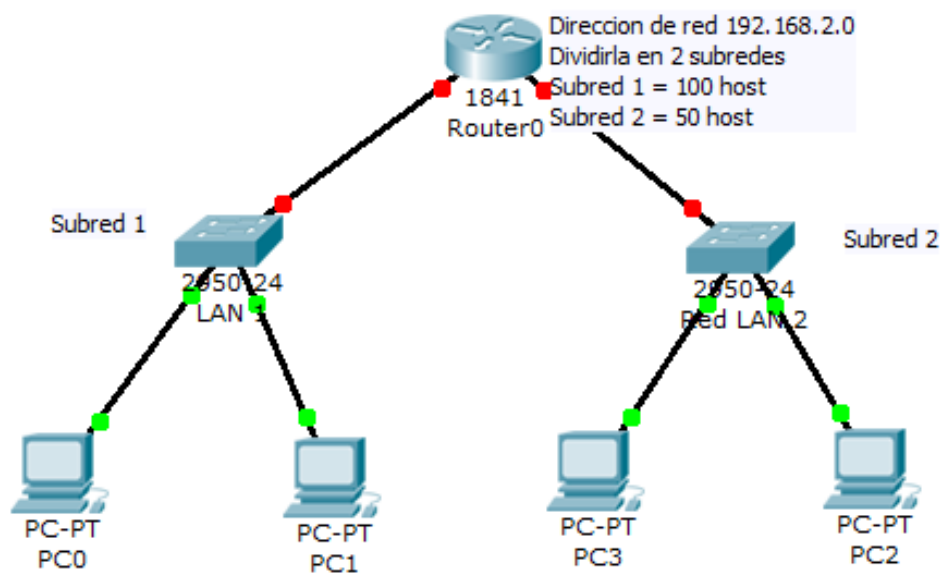
Actividad 1: Complete los siguientes cuadros calculando los valores a partir de los números dados utilizando VSLM (Variable Length Subnet Masking)

Numero de subredes usables	14	1000	6	6	126	2000
Numero de host usables	14	60	30	30	131,070	15
Dirección de red	192.10.10.0	165.100.0.0	210.100.56.0	195.85.80.0	118.0.0.0	178.100.0.0
Clase de mascara de subred						
Mascara de subred variada						
Numero de bits prestados						

Numero de subredes usables	1	60	2	250	5	
Numero de host usables	45	1000	60			25
Dirección de red	200.175.14.0	128.77.0.0	198.100.10.0	101.0.0.0	218.35.50.0	218.35.50.0
Clase de mascara de subred						
Mascara de subred variada						
Numero de bits prestados						

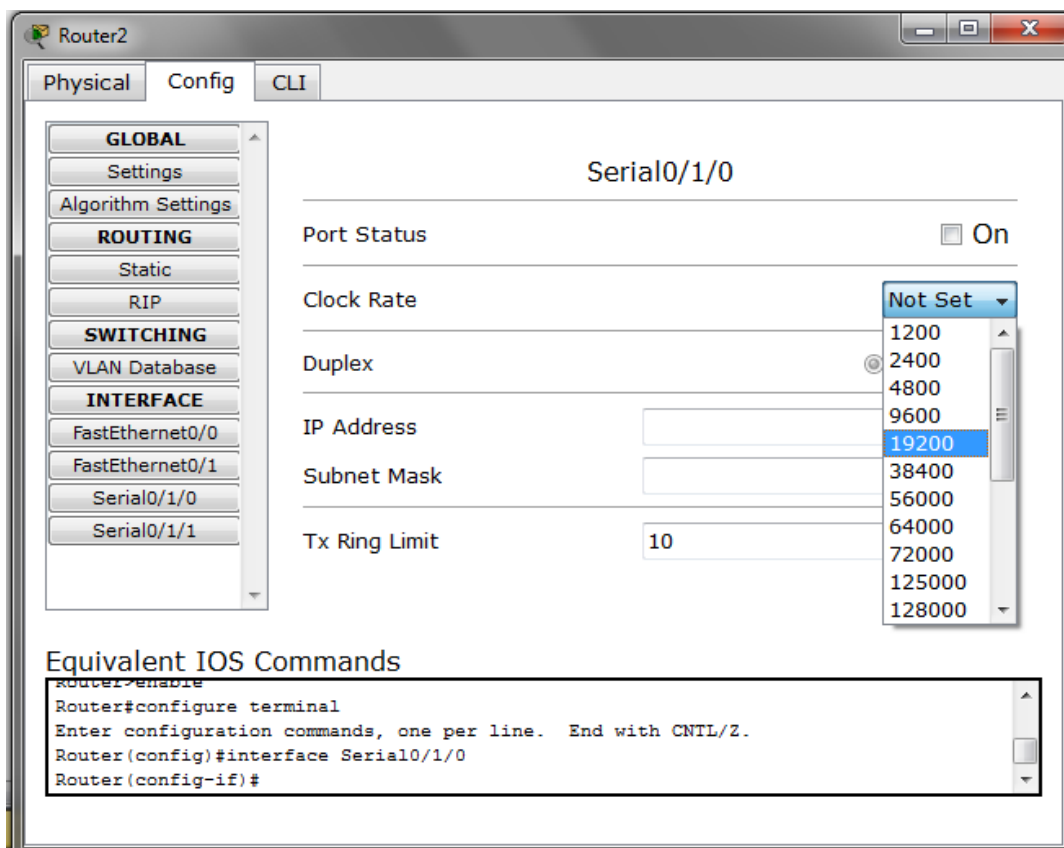
VII. Actividad 2: Realice los cálculos, asignación y configuración de los equipos necesarios para la simulación correcta de los siguientes escenarios.

Escenario 1. Subnetting de una red.





En este caso se debe tomar en cuenta la unión tipo WAN entre los routers. Es necesario para esta conexión apagar el router, luego agregar el módulo WIC-2AM y luego encender el router. Una vez realizado esto, se procede a utilizar un tipo de conexión DCE. En el extremo en donde se conecta la línea por primera vez se debe activar el puerto y establecer el clock rate como muestra la siguiente imagen.



Una vez realizado este proceso se asignan las direcciones static en la pestaña de routing. En estos cuadros se completa con la red que está conectado del otro extremo del router y su máscara de red. En cuanto al espacio de next hop, se agrega la dirección IP del otro punto de la conexión WAN.

VIII. Preguntas de control

1. ¿Qué tipo de línea se utiliza para conectar dispositivos no iguales?
2. ¿Qué tipo conector se utiliza para conectar 2 routers?
3. ¿Qué función realiza la configuración del routing?



IX. Trabajo previo

Realizar los cálculos pertinentes al diseño de las redes presentadas en los escenarios.



Laboratorio No. 8: Protocolos IP, TCP y UDP

Curso	Capacitación en telefonía IP		
Modulo	Redes de Datos	Grupo	
Tipo Practica	<input type="checkbox"/> Laboratorio <input type="checkbox"/> Simulación		
Unidad Temática			
No Alumnos por practica	1	Fecha	
Nombre del Profesor			
Nombre(s) del Alumno(s)			
Tiempo estimado	45 minutos	Vo. Bo. Del Docente	
Comentarios			

Objetivos de la práctica de laboratorio

I. Objetivo General

1. Analizar los campos y funcionamiento de los protocolos IP, TCP y UDP.

II. Objetivos específicos

1. Identificar los campos de los protocolo IP, TCP y UDP.
2. Comprender el proceso de conexión de sesión usado por TCP.
3. Mostrar las ventajas de un proceso no orientado a la conexión.

III. Medios a utilizar

- Equipo de computo
- Programa analizador de protocolos – Wireshark
- Conexión a internet

IV. Introducción

Este laboratorio se enfoca en el estudio de los protocolos de capa 3 como son IP, TCP y UDP. Los ejercicios que se presentan tienen la facilidad de mejorar la comprensión sobre los campos de cada uno de los protocolos. El encabezado IP es el más utilizado a nivel mundial, pues es válido por la sencillez y eficacia con que opera.



TCP es un protocolo orientado a la conexión, es comúnmente utilizado por todos los ordenadores conectados a Internet, de manera que éstos puedan comunicarse entre sí. El hecho de utilizar protocolos que inicia sesión de conexión da una mayor seguridad en el envío de datos. Sin embargo, este posee algunas desventajas al implementarlo a ciertos servicios.

UDP es un protocolo que permite el envío de datagramas a través de la red sin que se haya establecido previamente una conexión o sesión, ya que el propio datagrama incorpora suficiente información de direccionamiento en su cabecera. Este tipo de paquete resulta muy desventajoso ante ciertas aplicaciones. Sin embargo, es muy útil para servicios en tiempo real a diferencia que TCP.

V. Conocimientos previos

- Protocolo IP, TCP y UDP
- Manejo del analizador de protocolos

VI. Procedimiento

Actividad 1: Campos de protocolo IP

Paso 1: Inicie el programa analizador de protocolos Wireshark

Paso 2: Proceda a realizar la captura de paquetes y filtre los paquetes IP. Una vez realizado esto, abra el explorador de internet y cargue la página www.google.com.ni

Paso 3: Detenga la captura de paquetes.

Al realizar la filtración notara que los paquetes restantes no tienen en la casilla protocolo las letras IP.

¿Qué protocolos son mostrados en esta casilla luego de la filtración?



¿A qué se debe este resultado en la filtración?

Paso 4: Seleccione un paquete y vaya al panel de detalles del paquete. En este punto lograr ver los campos del encabezado IP del paquete.

¿Qué campos logra visualizar?

Según las flags del paquete IP, ¿cuáles son las características que posee el paquete seleccionado?



Actividad 2: Campos del protocolo TCP.

Paso 1: Con la misma captura realizada anteriormente, realice una filtración de protocolo TCP.

Paso 2: Observe que hay paquetes que no presentan las letras TCP en la casilla protocol.

Nombre dos protocolos que resultan en la lista de protocolos capturados según la filtración.

1. _____

2. _____

¿A qué se debe esto?

Actividad 3: Protocolo orientado a la conexión

Paso 1: Filtre nuevamente la lista de captura de paquetes con el protocolo HTTP.

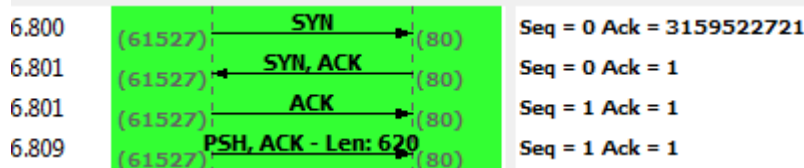
Paso 2: Ordene los protocolos de paquetes de forma alfabética y ubique los paquetes que muestran las letras HTTP en la casilla de **protocol**.

Paso 3: Seleccione el paquete HTTP que muestra en el campo **info** la expresión GET / HTTP/1.1

Paso 4: De click derecho sobre este paquete y establezca como filtro de conversación TCP.

Paso 5: A continuación genere un gráfico de flujo, usando esta opción en la ventana statistics.

Deberá obtener un gráfico similar al presentado a continuación.



¿Que son los mensajes SYN y ACK?

Explique brevemente el proceso de establecimiento de sesión y envío de datos entre host utilizando TCP.

Actividad 4: Campos de la unidad de datagrama

Paso 1: Realice un filtrado general de la lista de paquetes utilizando el protocolo UDP.

Paso 2: Ordene de forma alfabética los paquete dando click izquierdo sobre la pestaña protocol

Paso 3: ubique los paquetes que contienen las letras UDP en el campo protocol.

Paso 4: Busque en el panel de detalle de paquetes la sección de UDP

¿Qué campos presenta el protocolo de unidad de datagrama UDP?

Actividad 5: Envío y recepción de datagramas

Retome la práctica en el último paso de la actividad anterior.



Paso 1: Una vez filtrada la conversación, procesa a generar un gráfico de flujo a fin de observar el envío de los datagramas de un host a otro.

¿Qué sucede en el envío de datagramas?

¿Existen mensajes de respuesta o confirmación ACK, por aparte del receptor?

VII. Preguntas de control

1. ¿Qué es un protocolo orientado a la conexión?
2. ¿Cuáles son ventajas y desventajas de los protocolos no orientados a la conexión?
3. ¿Qué diferencias existen entre TCP y UDP?

VIII. Trabajo previo

Investigar: Ventana de recepción de paquetes
Establecimiento de sesión TCP
Gama de protocolos IP



Laboratorio No. 9: Protocolo de enrutamiento OSPF.

Curso	Capacitación en telefonía IP		
Modulo	Redes de Datos	Grupo	
Tipo Practica	<input type="checkbox"/> Laboratorio <input type="checkbox"/> Simulación		
Unidad Temática			
No Alumnos por practica	1	Fecha	
Nombre del Profesor			
Nombre(s) del Alumno(s)			
Tiempo estimado	75 minutos	Vo. Bo. Del Docente	
Comentarios			

Objetivos de la práctica de laboratorio

I. Objetivo General

1. Comprender el funcionamiento del protocolo OSPF de forma práctica.

II. Objetivos específicos

1. Realizar una configuración básica de red basada en OSPF.
2. Establecer parámetros de costes e intervalo de mensajes hello.
3. Configurar los equipos para establecer comunicación multi- áreas.

III. Medios a utilizar

- Equipo de computo
- Programa simulador de redes IP – Packet tracer
- Calculadora.

IV. Introducción

Open Short Path First versión 2, es un protocolo de routing interno basado en el estado del enlace o algoritmo Short Path First, estándar de Internet, que ha sido desarrollado por un grupo de trabajo del Internet Engineering task Force, cuya especificación viene recogida en el RFC 2328.



OSPF, ha sido pensado para el entorno de Internet y su pila de protocolos TCP/IP, como un protocolo de routing interno, es decir, que distribuye información entre routers que pertenecen al mismo Sistema Autónomo.

OSPF es la respuesta de IAB a través del IETF, ante la necesidad de crear un protocolo de routing interno que cubriera las necesidades en Internet de routing interno que el protocolo RIP versión 1 ponía de manifiesto:

- Lenta respuesta a los cambios que se producían en la topología de la red.
- Poco bagaje en las métricas utilizadas para medir la distancia entre nodos.
- Imposibilidad de repartir el tráfico entre dos nodos por varios caminos si estos existían por la creación de bucles que saturaban la red.
- Imposibilidad de discernir diferentes tipos de servicios.
- Imposibilidad de discernir entre host, routers, diferentes tipos de redes dentro de un mismo Sistema Autónomo.

Algunos de estos puntos han sido resueltos por RIP versión 2 que cuenta con un mayor número de métricas así como soporta CIRD, routing por subnet y transmisión multicast.

Dado que el enrutamiento OSPF depende del estado de enlace entre dos routers, los vecinos deben reconocerse entre sí para compartir información. Este proceso se hace por medio del protocolo Hello.

Un router se ve a sí mismo listado en un paquete Hello que recibe de un vecino.

Los paquetes se envían cada 10 segundos (forma predeterminada) Utilizando la dirección de multidifusión 224.0.0.5. Para declarar a un vecino caído el router espera cuatro veces el tiempo del intervalo Hello (intervalo Dead).

En redes con difusión se lleva a cabo la elección de DR y BDR. Los routers de un entorno multiacceso, como un entorno ethernet, deben elegir un



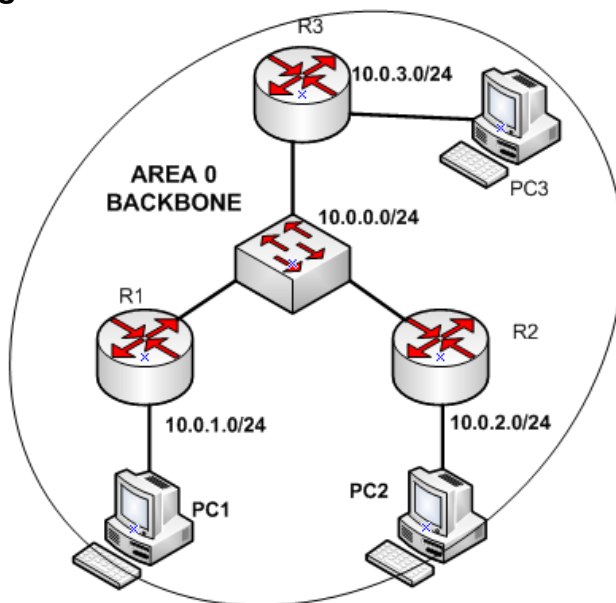
Router Designado (DR) y un Router Designado de Reserva (BDR) para que representen a la red. Un DR lleva a cabo tareas de envío y sincronización. El BDR solo actuara si el DR falla. Cada router debe establecer una adyacencia con el DR y el BDR.

V. Conocimientos previos

- Concepto OSPF
- Mensaje Hello en OSPF
- Conocimiento sobre áreas OSPF

VI. Procedimiento

Actividad 1. Configuración básica en un área OSPF



Paso 1. Inicie el programa Packet Tracer. Proceda a construir la red que se muestra en la figura anterior.

Paso 2. Complete la siguiente tabla diseñando así las redes. Acorde a lo establecido en la imagen anterior.

Dispositivo	Interfaz	Dirección IP	Mascara de red	Gateway
-------------	----------	--------------	----------------	---------



R1	Fa 0/0			
R1	Fa 0/1			
R2	Fa 0/0			
R2	Fa 0/1			
R3	Fa 0/0			
R3	Fa 0/1			
PC 1	Ethernet			
PC 2	Ethernet			
PC3	Ethernet			

Paso 3. Configure los dispositivos según los valores calculados en la tabla anterior.

Paso 4. Uso del comando “router OSPF”

Ahora es necesario utilizar el comando router ospf “*identificador de proceso*”. Este permite crear un proceso OSPF en el router. Es de gran importancia cuando se tienen múltiples procesos en el mismo router, este número es elegido por el administrador de red.

Como parte del protocolo, las redes deben anunciarse entre sí para lo cual utilizan el comando **network** “*ID de la red*” “*wildcardmask*” **área** “*id del área*”. El comando “network” indica a las interfaces que van a enviar o procesar mensajes de encaminamiento.

El campo wildcardmask es el complemento de la máscara de red, es decir, si la máscara es 255.255.255.0; la wildcardmask es 0.0.0.255.

A continuación se presentan los comandos necesarios para configurar el protocolo OSPF en el router R1.

R1# configure terminal



```
R1 (config)# router ospf 1
R1 (config - router)# network 10.0.0.0 0.0.0.255 area 0
R1 (config - router)# network 10.0.1.0 0.0.0.255 area 0
R1 (config - router)# ^Z
R1# show ip route
```

El último comando le permitirá revisar que las configuraciones hechas sean correctas.

Paso 5: Repita el mismo proceso con los parámetros correctos para los router R2 y R3.

Paso 6: verifique que la red funcione enviando mensajes ICMP entre los PCs, usando el comando Ping.

Actividad 2. Modificaciones al protocolo OSPF.

Paso 1:

Cada router escoge como identificador de router OSPF la dirección IP mayor. Si la interfaz que tiene ese dispositivo cae, es necesario cambiar la identificación de este router OSPF, cosa que puede afectar a la elección del DR y BDR. Para evitar este efecto, se suele configurar siempre una interfaz loopback con una dirección IP que no tiene por qué estar en el rango 127.0.0.0/8.

Para realizar dicho cambio se utilizan los siguientes comandos:

```
R1 (config)# interface loopback 0
R1 (config - if)# ip address 172.5.5.2 255.255.255.0
R1 (config - if)# exit
```

Paso 2:



Se pueden modificar también la prioridad de un router con el comando “**ip ospf priority number**”, donde “number” es un número entre 1 y 255. Prioridad 0 implica que el router no puede ser elegido DR o BDR, el valor por defecto es 1 y a mayor valor el router es elegido como DR o BDR.

La métrica por defecto usada en OSPF es el ancho de banda. En un router CISCO el coste de un enlace se calcula como $10^8/(\text{ancho de banda} - \text{bps})$. Por ejemplo si tenemos un enlace Ethernet a 10 Mbps el coste sería $10^8/10^7=10$, mientras que un modem a 56 Kbps tendría un coste de $10^8/56*10^3=1785$. El SPF es un algoritmo de mínimo coste. Podemos modificar el coste de un enlace de dos maneras:

Modificando el valor del coste en la interfaz de ese enlace con el comando “**ip ospf cost**” donde cost tiene un valor entre 1 y 65535 o (2) modificando el valor del ancho de banda en la interfaz que permite calcular el coste con el comando “**bandwidth value**”. Se debe remarcar que se está cambiando la velocidad real del enlace, solo el coste de cara a calcular el camino más corto.

La programación de esto se realizar a través de la siguientes líneas de comandos en una interfaz de tipo serial.

```
R1 (config)# interface s0
R1 (config - if)# bandwidth 2048000    ***2,048 Mbps***
R1 (config - if)# ip ospf cost 488      *** equivalente al comando anterior***
```

Paso 3:

Se pueden cambiar los valores de periodicidad de los temporizadores de paquetes Hello: hello-interval (tiempo entre paquetes hello, por defecto es 10 s) y dead-interval (tiempo que considera que el enlace ha caído, por defecto es 40 s). Los



temporizadores se modifican por interfaz con los comandos “**ip ospf hello-interval value**” y “**ip ospf dead-interval value**”

Los comandos son:

R1 (config –if)# ip ospf hello – interval 30

R1 (config – if)# ospf dead – interval 120

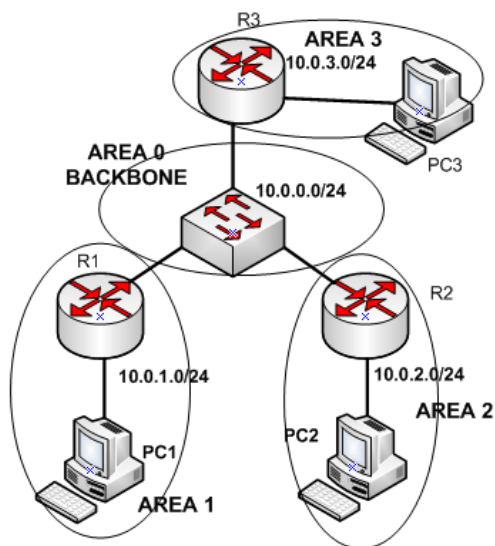
R1 (config – if)#^Z

Paso 4.

Sustituya el switch de la configuración anterior por enlaces WAN de tipo serial y proceda a realizar las configuraciones mostradas en los pasos 1,2 y 3 de la actividad 2.

Actividad 3. Configuración de áreas múltiples

La siguiente imagen muestra la interconexión de distintas redes y cada una de ellas se configura o interpreta como un área OSPF distinta.



Paso 1:



Si hay más de un área, siempre debe haber un área 0 que haga de backbone. Por lo cual se debe configurar el área de backbone (área 0) y a continuación el resto de áreas. Esto es el proceso utilizado en la estructura de redes jerárquicas.

A las rutas que se generan dentro de un área se les llama **intra-area-routes** y aparecerán en la tabla de enrutamiento identificadas con la letra **O**. A las rutas aprendidas de otra área se les llama **inter-area-routes** o **summary-routes** y aparecerán en la tabla de enrutamiento identificadas con la letra **O IA**. A las rutas inyectadas desde otros protocolos de encaminamiento (usando redistribución de rutas) se les llama **external-routes** y aparecerán en la tabla de encaminamiento identificadas con la letra **O E1** (tipo 1 significa que el coste es la suma del protocolo interno más el externo) o **O E2** (tipo 2 significa que el coste es siempre el del protocolo externo). Por defecto OSPF siempre redistribuye con tipo 2.

A continuación se muestra la configuración de del router R1 de la imagen anterior para esa misma red.

```
R1 (config)# interface fa 0/0
R1 (config - if)# ip address 10.0.1.0 255.255.255.0
R1 (config - if) # no shutdown
R1 (config - if) # exit
R1 (config) # interface fa 0/1
R1 (config - if) # ip address 10.0.0.1 255.255.255.0
R1 (config - if) # no shutdown
R1 (config - if) # exit
R1 (config) # router ospf 1
R1 (config - router) # network 10.0.0.0 0.0.0.255 area 0
R1 (config - router) # network 10.0.1.0 0.0.0.255 area 1
R1 (config - router) # ^Z
```

Paso 2: Realice el mismo proceso para los otros 2 router y luego verifique que exista comunicación en la red.



VII. Preguntas de control

1. ¿Qué es la wildcardmask?
2. ¿Qué es un DR y DBR?
3. ¿Cuáles la función del comando router OSPF?
4. ¿Cuáles son las ventajas de OSPF?
5. ¿Qué representa el coste en los router OSPF?
6. ¿Cómo se denominan las rutas que se generan dentro de un área OSPF?

VIII. Trabajo previo

- ✓ Leer sobre OSPF y sus áreas
- ✓ Calcular los parámetros de la tabla a utilizar en la sección 1.



Laboratorio No. 10: Protocolos ARP, ICMP, DHCP y HTTP.

Curso	Capacitación en telefonía IP		
Modulo	Redes de Datos	Grupo	
Tipo Practica	<input type="checkbox"/> Laboratorio <input type="checkbox"/> Simulación		
Unidad Temática			
No Alumnos por practica	1	Fecha	
Nombre del Profesor			
Nombre(s) del Alumno(s)			
Tiempo estimado	45 minutos	Vo. Bo. Del Docente	
Comentarios			

Objetivos de la práctica de laboratorio

I. Objetivo General

1. Comprender el funcionamiento de los protocolos ARP, ICMP, DHCP, DNS y HTTP.

II. Objetivos específicos

1. Identificar los campos del paquete ARP e ICMP.
2. Crear esquemas del proceso de los protocolos DHCP y DNS.
3. Utilizar las utilidades de la barra statistics en wireshark para visualizar el envío y recepción de paquetes.

III. Medios a utilizar

- Equipo de computo
- Programa analizador de protocolos – Wireshark
- Conexión a internet

IV. Introducción

El laboratorio a desarrollar el estudio de protocolos para implementación de servicios y funcionamiento de la red local. Los protocolos ARP e ICMP tiene la finalidad de articular las distantes partes de la red LAN para que esta opere correctamente. Se muestra la utilidad de algunos comandos como ping y nslookup como herramientas para probar la conectividad entre puntos.



Los protocolos DNS y DHCP brindan los servicios de conversión de direcciones lógicas o textuales a conversiones de octetos y asignación dinámica de direcciones IP, respectivamente. La importancia del protocolo DNS surge con el crecimiento y aumento de páginas web, pues resulta más sencillo recordar nombres a una serie numérica por página. El DHCP facilita la configuración de los ordenadores, disminuyen el número de errores que se pueden generar al configurar de forma estática un cantidad grande de ordenadores.

El último protocolo de estudio es el HTTP, que permite la transferencia y manipulación de texto relacionado con links hacia otras páginas web. Este protocolo es conocido como protocolo de transferencia de hyper-texto.

V. Conocimientos previos

- Protocolo ARP
- Protocolo ICMP
- Protocolo HTTP
- Protocolo DNS
- Protocolo DHCP.
- Manejo del analizador de protocolos

VI. Procedimiento

Actividad 1. Análisis de paquete ARP

Paso 1. Inicie en analizar de protocolos Wireshark y proceda a comenzar la captura de paquetes.

Paso 2. Una vez iniciado el proceso de captura filtre los paquetes ARP.

Paso 3. Detenga el proceso de captura de paquetes y seleccione uno de los paquetes ARP.



Paso 4. A continuación proceda a completar las siguientes preguntas.

¿Qué longitud posee la trama?

¿Cuál es su dirección de IP de origen y destino?

¿Cuáles son las direcciones MAC de origen y destino del paquete ARP?

¿Cuáles son los posibles tipos de mensajes ARP?

Actividad 2. Análisis de paquete ICMP

Paso1. Inicie el analizador de puertos y comience el proceso de captura de paquetes. Recuerde desactivar la pestaña de Captura de paquetes en modo promiscuo.

Paso2. Abra la dirección Ejecutar/Cmd y a continuación usaremos el comando ARP – A, de tal forma que podamos ver las otras direcciones IP en uso.

Paso3. Realizaremos un envío de paquetes de prueba con el comando ping a una de las direcciones IP que se muestran en la tabla ARP.

Paso4. Detenga la captura de paquetes y proceda a filtrar los paquetes ICMP.

Paso 5. Responda las siguientes preguntas.

¿Cuál es la longitud de la trama?



¿Cuáles son la dirección IP de origen y destino? ¿Corresponden a las direcciones de la su PC y PC remota?

Inicie una nueva captura de paquetes y regrese a la ventana cmd. Una vez ahí utilice el comando `ping /?` y busque la opción que le permita modificar el tamaño del paquete y modifíquelo. Utilice el comando `ping` para enviar paquete con mayor bytes.

Verifique utilizando el analizador de protocolos que el tamaño de los datos enviados en los paquetes ha variado.

Actividad 3. Análisis de paquetes DNS

Paso 1. Inicie el proceso de captura de paquetes. Recuerde desactivar la opción de recepción de paquetes en modo promiscuo.

Paso 2. Ahora inicie nuevamente la ventana Ejecutar/cmd. Usaremos el comando `nslookup` lo que nos permite solicitar a nuestro servidor de nombre de dominio las direcciones ip de los servidores que almacenan esa página web. Solicite la dirección IP de 2 páginas web.

Paso3. Finalice el proceso de captura y filtre los paquetes que utilizan el protocolo DNS.

Paso 4. De click en la pestaña protocolo y agrupe todos los protocolos que muestran en la casilla de protocolos DNS.

Paso 5. Responda las siguientes preguntas.



¿Cuáles son los parámetros que se muestran dentro del campo DNS en el analizador?

¿En cuántos intentos logro dar respuesta el servidor DNS?

Paso 6. Reinicie la captura de paquetes y escriba una dirección web que no tenga página o servidor.

Paso 7. Detenga la captura, filtre el protocolo DNS y agrupe los paquetes.

Paso 8. Observe que sucede con los paquetes que son enviados con la solicitud de la página que escribió y realice un esquema que muestre el proceso.

Actividad 3. Análisis de protocolo DHCP

Paso 1. Inicie la captura de paquetes.

Paso 2. Abra la ventana Ejecutar/cmd

Paso 3. Libere el ip de la máquina que utiliza escribiendo el comando ipconfig /release seguido del comando ipconfig /renew. En este punto el ordenador ha perdido su dirección IP y está solicitando una nueva.

Paso 4. Regrese al analizador de puertos y detenga la computadora. Agrupe los protocolos por orden alfabético y ubique los paquetes con protocolos DHCP.



Paso 5. Proceda a realizar un gráfico donde se muestren las partes del dialogo entre las terminales acorde a los resultado de la captura.

Actividad 4. Análisis de protocolo HTTP.

Paso 1. Inicie la captura de paquetes.

Paso 2. Utilizando el buscador de internet de su preferencia cargue la página www.google.com.ni.

Paso 3. Detenga la captura de paquete, filtre los paquetes http. Luego proceda a generar un gráfico sobre el intercambio de paquetes haciendo uso de la herramienta gráfico de flujo y la pestaña estadísticas.

Paso 4. Explique brevemente que sucede en cada envió o recepción.

VII. Preguntas de control

1. ¿Cuál es la función del DHCP?
2. ¿Cuáles son los elementos del paquete DNS?
3. ¿Cuál es la función del mensaje ICMP?
4. ¿Cuáles son los mensajes HTTP que se envían antes de iniciar la transferencia de datos?

VIII. Trabajo previo

- ✓ Investigar sobre el funcionamiento de protocolos ARP, ICMP, DNS, DHCP y HTTP.
- ✓ Leer sobre servidores DNS y su función.
- ✓ Leer sobre las fases en el proceso de adquisición de una IP para computadoras.



Laboratorio No. 11: Introducción al simulador de red grafico GSN3.

Curso	Capacitación en telefonía IP		
Modulo	Redes de Datos	Grupo	
Tipo Practica	<input type="checkbox"/> Laboratorio	<input type="checkbox"/> Simulación	
Unidad Temática			
No Alumnos por practica	1	Fecha	
Nombre del Profesor			
Nombre(s) del Alumno(s)			
Tiempo estimado	75 minutos	Vo. Bo. Del Docente	
Comentarios			

Objetivos de la práctica de laboratorio

I. Objetivo General

1. Adquirir habilidades en el manejo del simulador GSN3..

II. Objetivos específicos

1. Presentar el simulador de redes gráfico y sus paneles de herramientas
2. Conocer las funciones y herramientas brindadas por el simulador
3. Facilitar el estudio del simulador a través de ejemplos prácticos.

III. Medios a utilizar

- Equipo de computo
- Programa simulador de redes GSN3
- Paquete de complementos Dynamips, Microcore de Linux e IOS de routers.

IV. Introducción

GNS3 es un simulador gráfico de redes que le permitirá diseñar fácilmente topologías de red y luego ejecutar simulaciones en él. Hasta este momento GNS3 soporta el IOS de routers, ATM/Frame Relay/switchs Ethernet y PIX firewalls.

El simulador permite extender la red real propia, conectándola a la topología virtual. Para realizar esto, GNS3 está basado en Dynamips, PEMU (incluyendo el



encapsulador) y en parte en Dynagen, que fue desarrollado en python a través de PyQt la interfaz gráfica (GUI) confeccionada con la poderosa librería Qt, famosa por su uso en el proyecto KDE. GNS3 también utiliza la tecnología SVG (Scalable Vector Graphics) para proveer símbolos de alta calidad para el diseño de las topologías de red.

Dynamips es un emulador de routers Cisco escrito por Christophe Fillot. Emula a las plataformas 1700, 2600, 3600, 3700 y 7200, y ejecuta imágenes de IOS estándar.

Según Christophe Fillot, este tipo de emulador es útil para:

- Ser utilizado como plataforma de entrenamiento, utilizando software del mundo real.*
- Permite a la gente familiarizarse con dispositivos Cisco.*
- Probar y experimentar las funciones del Cisco IOS.*
- Verificar configuraciones rápidamente que serán implementadas en routers reales*

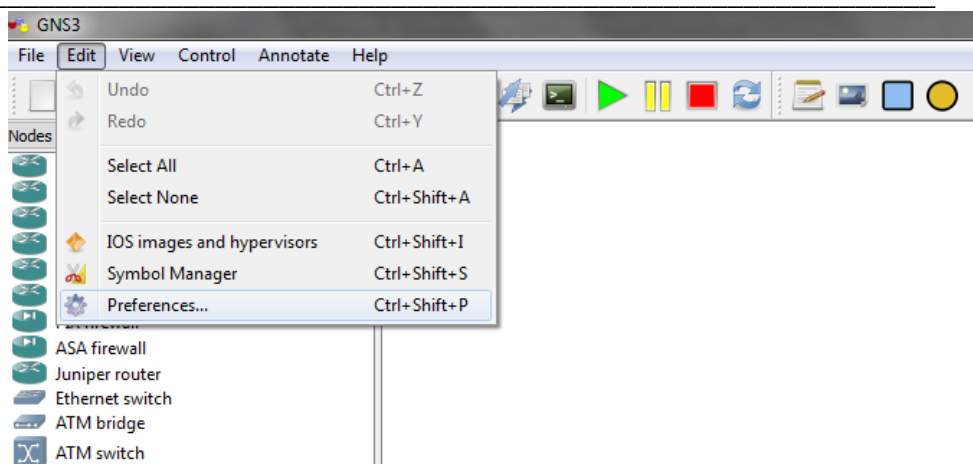
V. Conocimientos previos

- Configuración física y lógica de redes IP.
- Configuración básica de routers.
- Dynamips

VI. Procedimiento

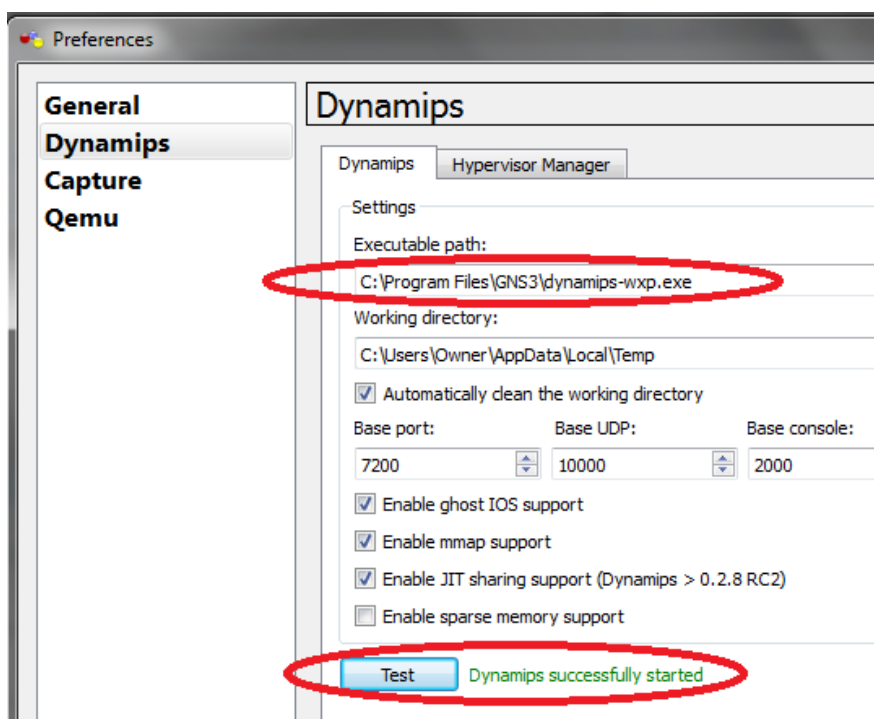
Actividad 1. Configuración de Dynamips

Paso 1. Inicie el programa GSN3 y ubique la pestaña Edit > Preferences.



Paso 2. . De click en la opción de Dynamips.

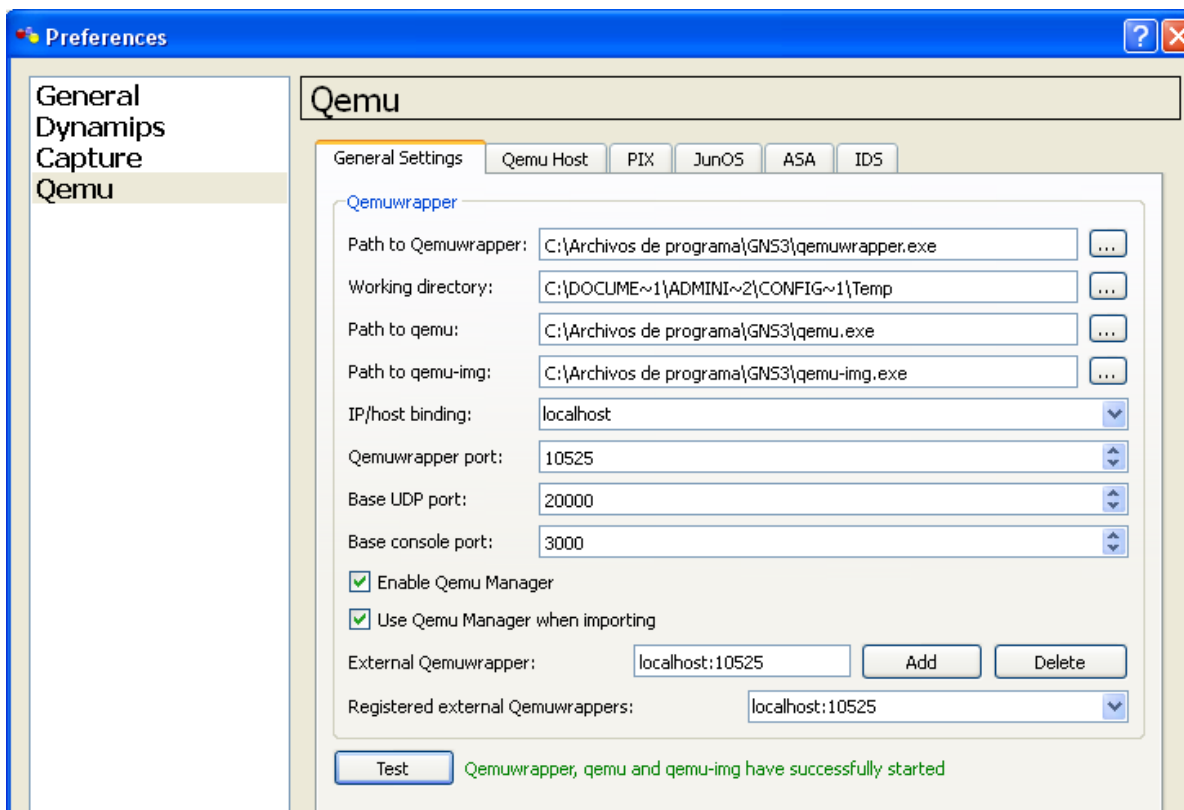
En esta parte deberá seleccionar el camino hacia al archivo ejecutable de Dynamips como se muestra en la siguiente figura. Una vez, que haya seleccionado el archivo de probar que este funcione correctamente dando click en la opción “Test”.



Actividad 2. Configuración de Qemu Host.

Los qemu host son ordenadores virtuales que operan con OS tipo Linux. EN este programa es necesario el uso de versiones reducidas de Linux para que el programa pueda manejarlos.

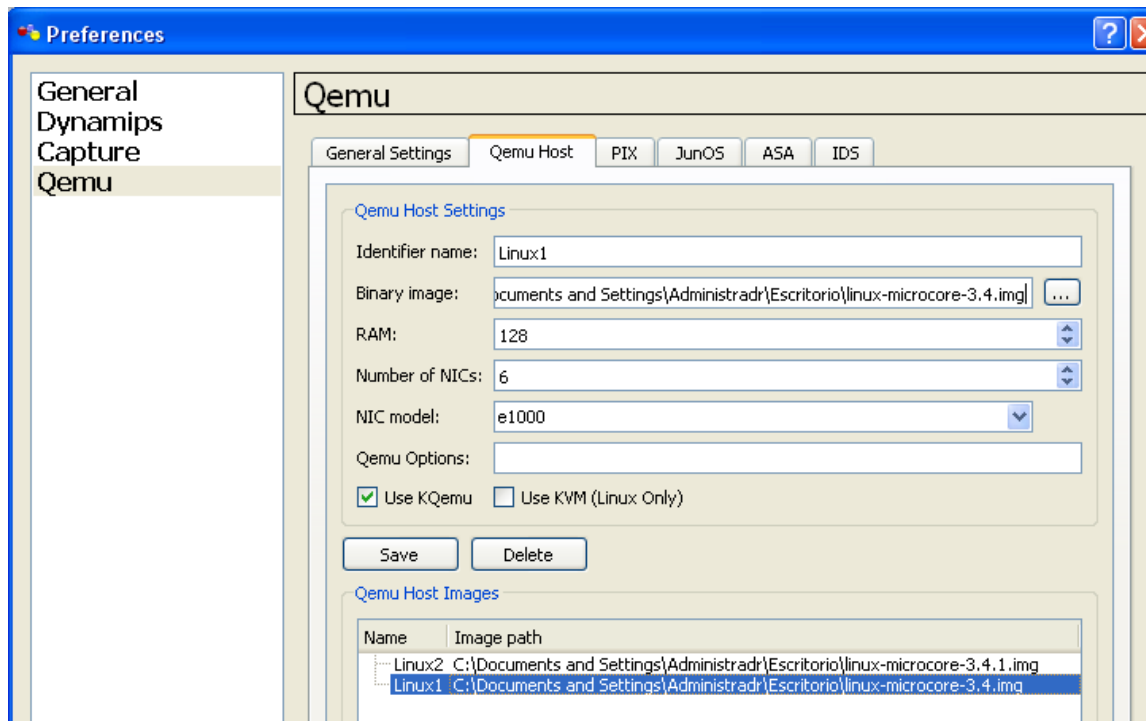
Paso 1. Vaya a la pestaña edit.>preference>qemu>General Settings, como se muestra en la siguiente figura.



- Las opciones path to Qemuwrapper y Working directory, definen parámetros para el funcionamiento del emulador de terminal.
- Path to qemu, define la ruta hasta el archivo ejecutable del emulador.
- Path to qemu-img, establece la línea de trayecto hasta la imagen del emulador.

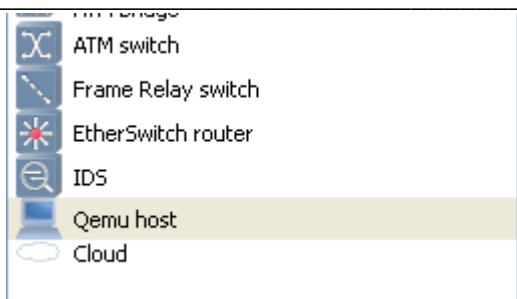
- Una vez configurados estos parámetros se da click en la pestaña Test, los cual determina si los parámetros y archivos configurados, funcionan correctamente.

Paso 2. Luego se configura el nombre de los qemu a utilizar, y se cargan las imágenes de Microcores de Linux para cada Qemu.

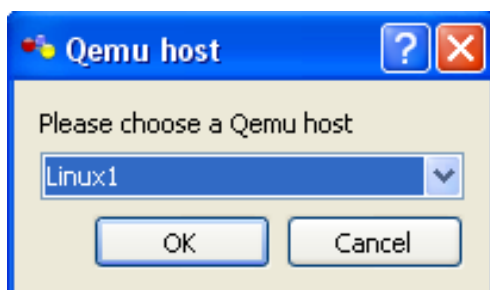


- El identifier name, permite asignar al qemu un nombre.
- La sección binary image, contiene la dirección hacia la imagen de microcore de Linux a utilizar. Si es necesario utilizar varios Qemus se recomienda hacer copias de los microcores, cada qemu debe tener si propio micro núcleo Linux.
- NIC model, determina el modelo de la tarjeta de red que se desea utilizar.

Paso 3. Proceda a tomar un Qemu host de la barra de nodos.

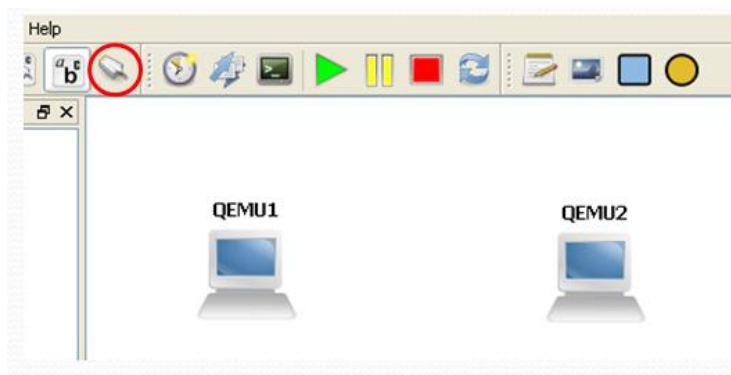


Paso 4. En la ventana emergente seleccione una de las imágenes de microcore de Linux que se cargaron previamente.



Realice el mismo proceso para establecer el próximo Qemu.

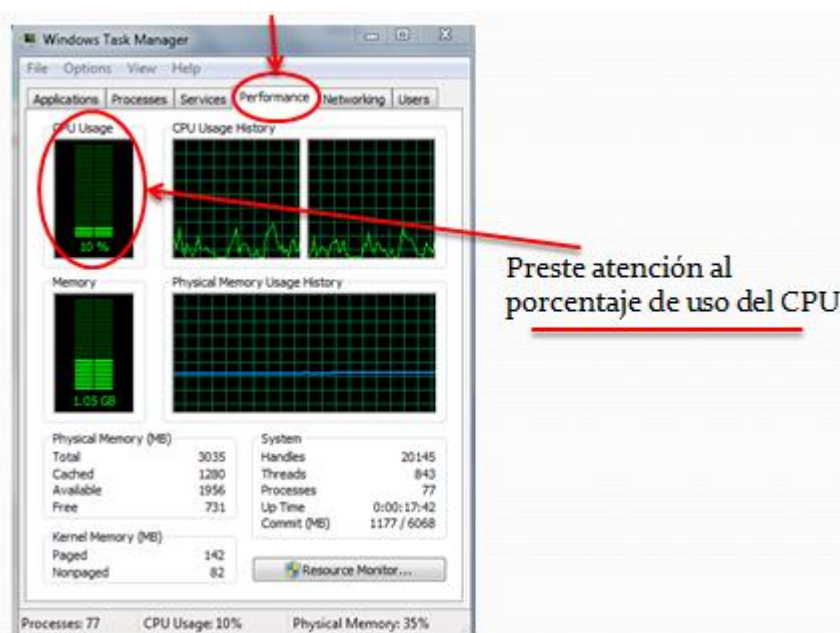
Paso 5. Haciendo uso del icono de “Crear un enlace” procedemos a unir los Qemu host.



En esta ventana seleccionaremos la opción “Manual”, no obstante al dar click sobre cada host deberemos seleccionar el puerto de interfaz ethernet que se desea conectar.

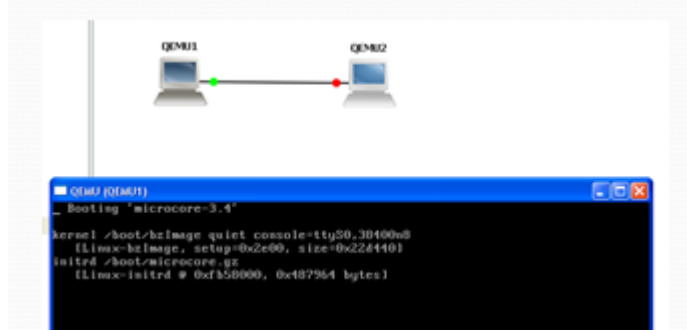


Paso 6: Inicie el administrador de tareas de Windows y seleccione la pestaña “rendimiento – performance”.



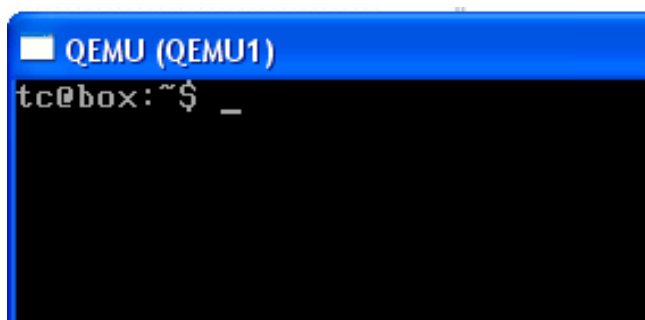
Paso 7: Inicie uno de los host permitiendo así que cargue el microcore de Linux.

Nota: observe como ha cambiado el porcentaje de uso de CPU al iniciar el microcore de Linux.



Se debe cargar un Qemu host a la vez.

Una vez que el microcore de Linux haya cargado obtendremos una ventana como la mostrada en la siguiente figura.



Paso 8: Utilice el comando “sudo su”, para iniciar el modo privilegiado en el Qemu host. En este modo asignaremos un nombre al host a través del comando “hostname”



Paso 9: A continuación procederemos a configurar las direcciones IP, mascara y estado de puerto en el Qemu host.



```
root@PC1:~# ifconfig eth0 192.168.2.1 netmask 255.255.255.0 up
root@PC1:~#
```

Define el comando para configurar los parámetros IP

Determina que puerto ethernet se esta configurando

Dirección IP del puerto

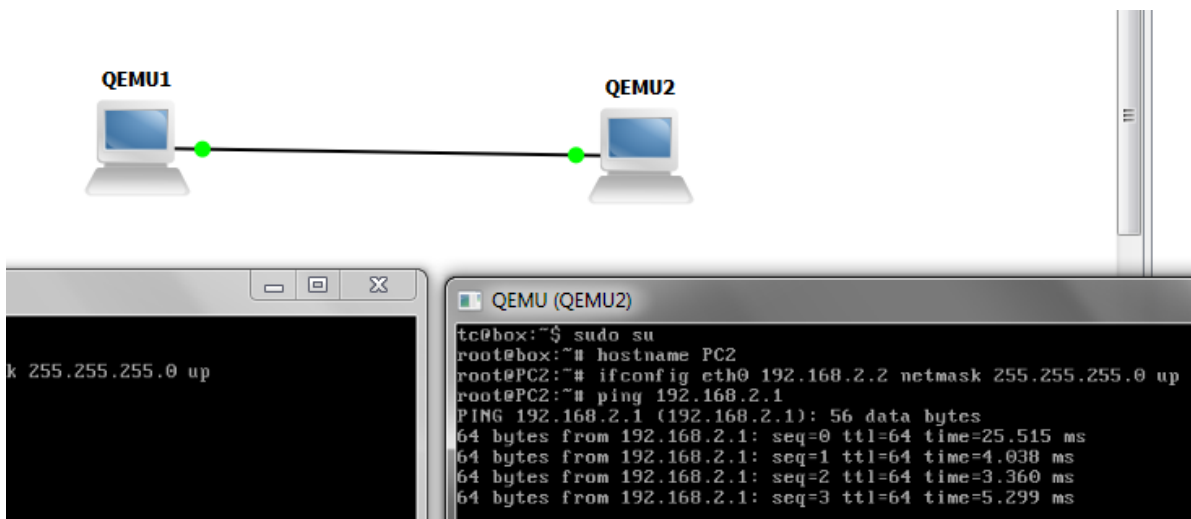
Define el comando para establecer la mascara de red

Código de mascara de red

Establece estado del puerto o terminal

Realice el mismo procedimiento para la PC2.

Paso 10: Utilizando el comando ping verifique que existe comunicación entre los Qemu host.



Para detener el proceso de envio de peticiones Ping presione Ctrl + C

Paso 11: Establecer el Gateway de la red.



```
root@box:~# ifconfig eth0 192.168.1.2 netmask 255.255.255.0 up
root@box:~# routing table
sh: routing: not found
root@box:~# route
Kernel IP routing table
Destination      Gateway          Genmask         Flags Metric Ref    Use Iface
127.0.0.1        *               255.255.255.255 UH    0      0      0 lo
192.168.1.0      *               255.255.255.0  U    0      0      0 eth0
root@box:~# route add default gw 192.168.1.1
root@box:~# route
Kernel IP routing table
Destination      Gateway          Genmask         Flags Metric Ref    Use Iface
127.0.0.1        *               255.255.255.255 UH    0      0      0 lo
192.168.1.0      *               255.255.255.0  U    0      0      0 eth0
default          192.168.1.1     0.0.0.0         UG    0      0      0 eth0
root@box:~# _
```

Muestra la tabla de enrutamiento del Que host

No se muestra el gateway por defecto

Permite agregar el gateway de la red

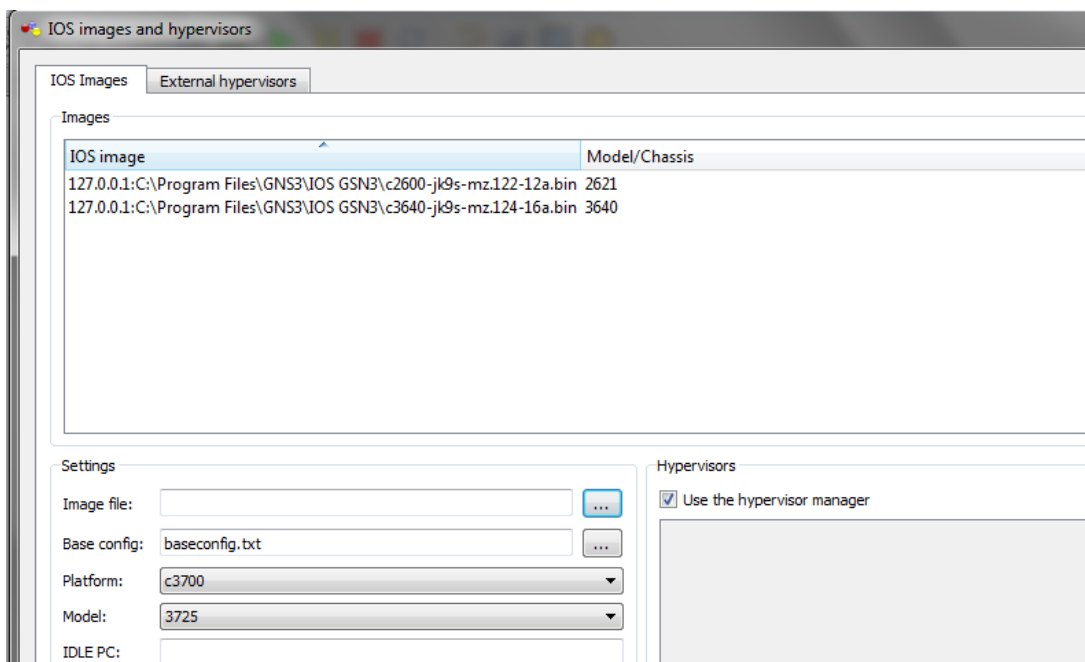
El gateway a sido agregado

Actividad 3. Prueba básica del simulador.

Paso 1. Verifique que el IOS del router C3640 ha sido cargado en el simulador.

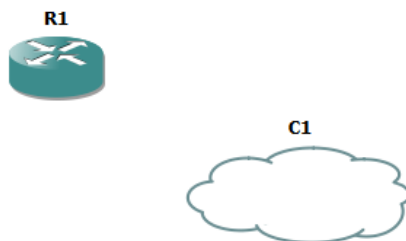
Esto se hace siguiendo la ruta Edit>IOS images and hypervisors. Si no han sido cargados deberá agregarlos.

La siguiente imagen muestra que los IOS a utilizar ya han sido cargados y pueden ser ocupados en la práctica.

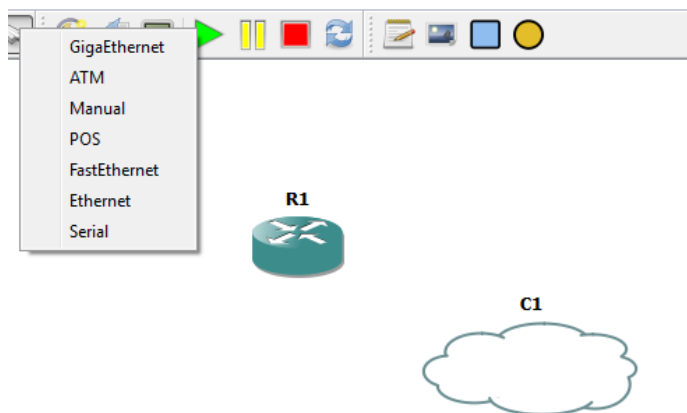




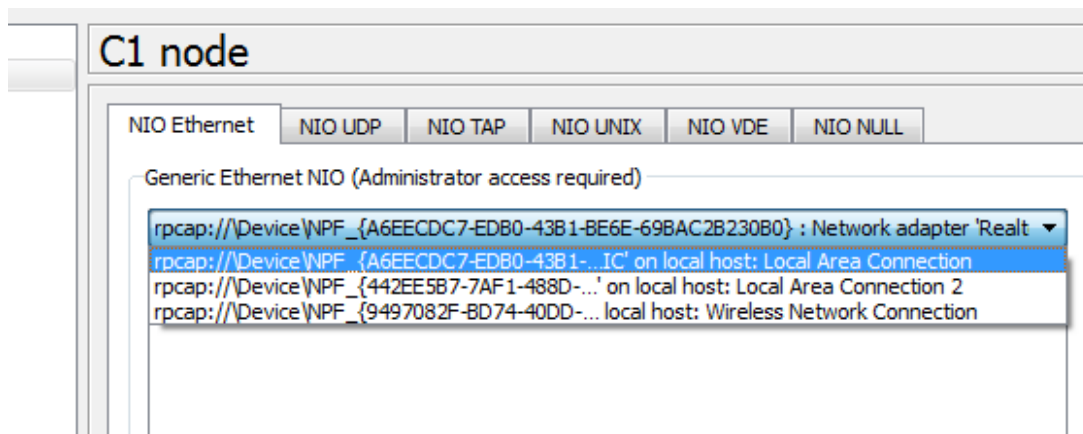
Paso 2. Tome un router C3640 y el icono de nube. Coloquelos en el panel de diseño.



Paso 3. Seleccione el icono de “agregar un enlace” y seleccionaremos la opción fastethernet.



Paso 4. Configure una entrada del nodo cloud.

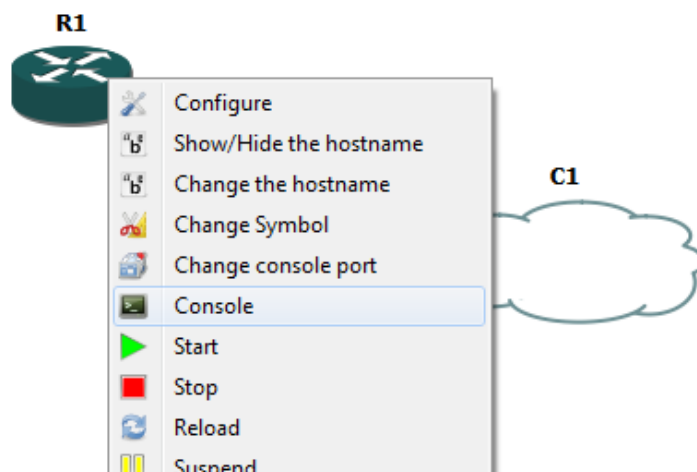


a) Click derecho sobre la nube y luego entre a configuración.



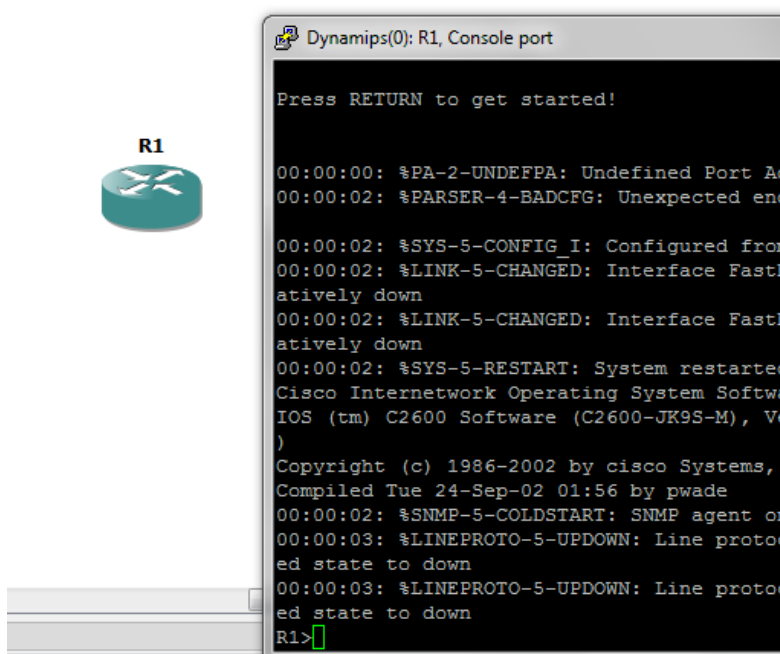
- b) Seleccione el interfaz que desea utilizar.
- c) Para observar estas opciones es necesario iniciar el programa en función de administrador.

Paso 5. Configuración del router.



Para ello es necesario iniciar el router y seleccionamos la opción “consola”.

Se abrirá una ventana del programa Putty que utiliza los dynamips para cargar la ventana de consola.





Nota: Pueden que en algunos casos sea necesario iniciar la ventana de consola previa a enlazar el router y cloud.

Paso 6: Configure el router acorde a los siguientes comandos.

```
R1>enable
R1#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z
R1(config)#hostname Prueba 1
      ^
% Invalid input detected at '^' marker.
R1(config)#hostname Prueba1
Prueba1(config)#
```

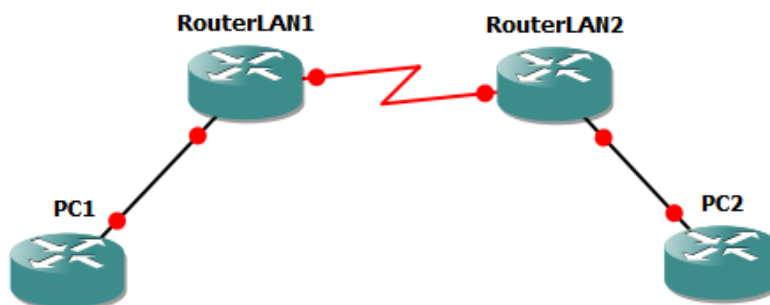
Paso 7: Configurando la terminal del router

```
Prueba1(config)#int fa0/0
Prueba1(config-if)#ip add 192.168.2.1 255.255.255.248
Prueba1(config-if)#no shutdown
Prueba1(config-if)#
```

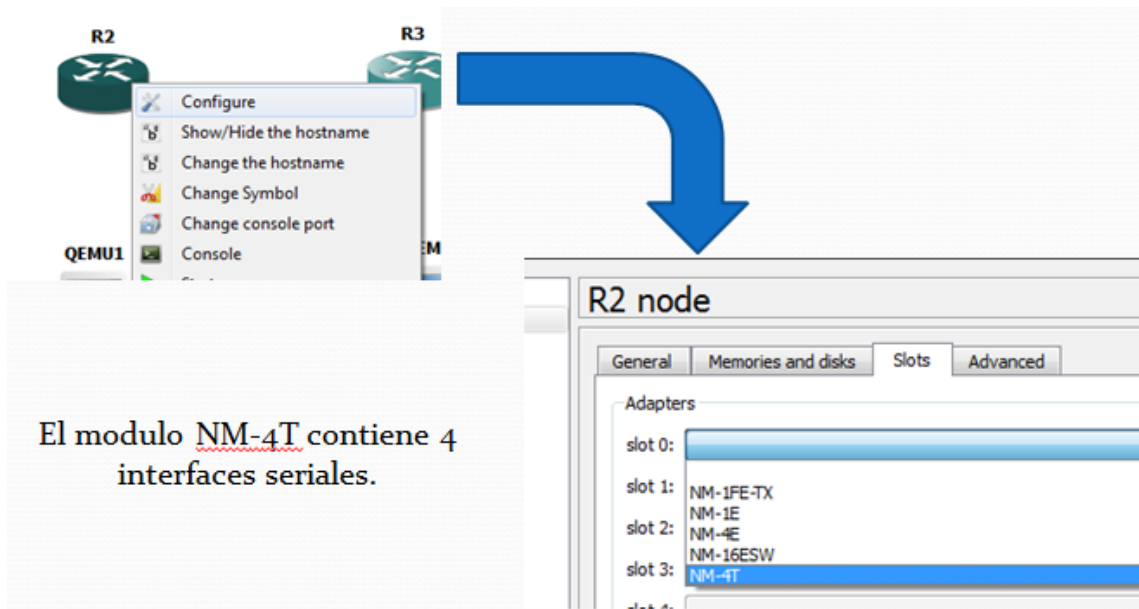
Para verificar que la dirección IP se ha configurado correctamente utilice el comando ping hacia esta misma.

Actividad 3: Interconexión de 2 redes LAN.

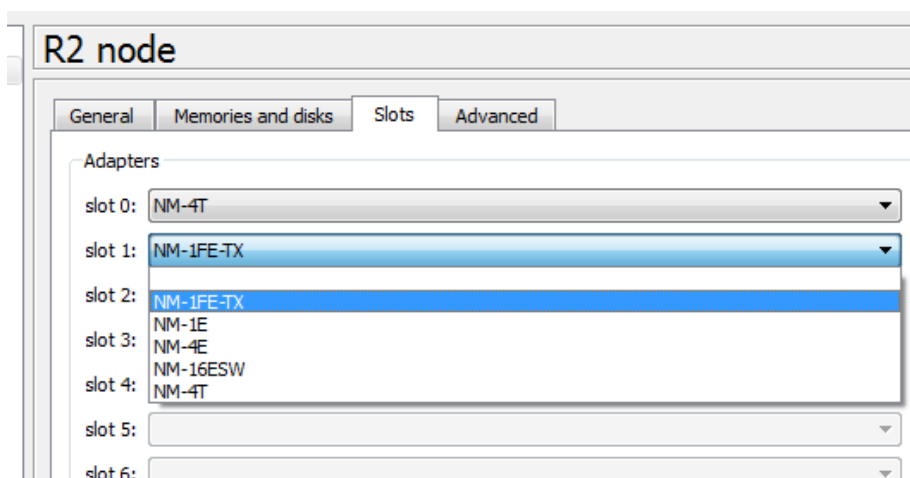
Paso 1. Forme los nodos que se muestran en la imagen a continuación y colóquelos en el panel de diseño.



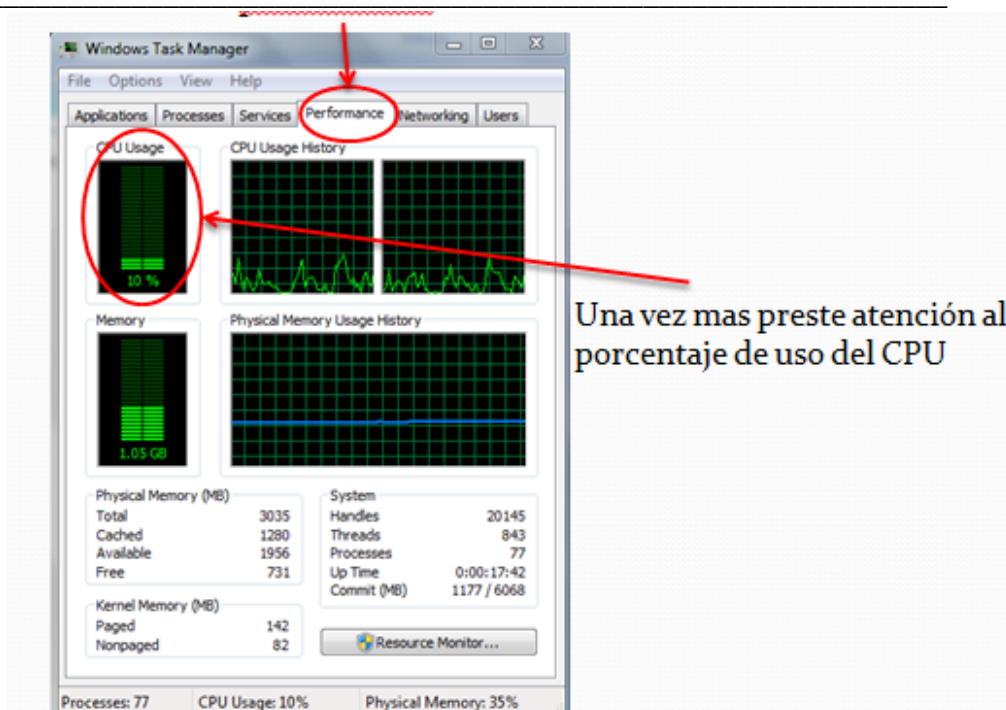
Paso 2: Agregue las interfaces seriales en cada router para conectarles posteriormente.



Paso 3: Agregue el módulo de conexión de interfaces FastEthernet.

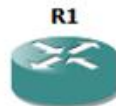


Paso 4: Inicie el administrador de tareas y Windows y seleccione la pestaña “rendimiento – perfomance”.




Paso 5: Inicie un router a la vez y utilice la opción de consola.


Para que funcione la opción de consola es necesario iniciar el router .



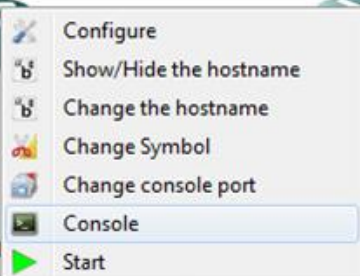
QEMU1



R2

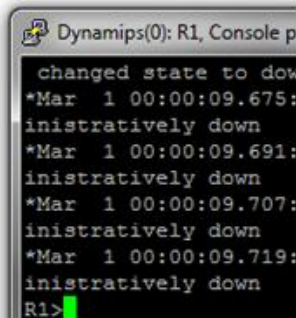


R3



QEMU1

QEMU2



Dynamips(0): R1, Console p

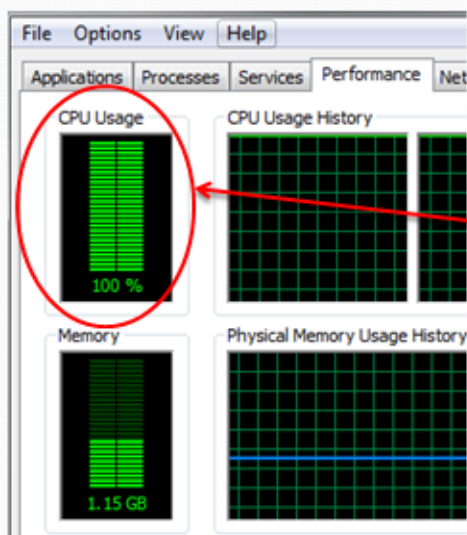
```

changed state to down
*Mar 1 00:00:09.675:
inistratively down
*Mar 1 00:00:09.691:
inistratively down
*Mar 1 00:00:09.707:
inistratively down
*Mar 1 00:00:09.719:
inistratively down
R1>

```

En esta ventana se cargara la imagen del IOS del router.

Observe el uso de CPU. Este valor puede resultar muy alto como en el ejemplo mostrado.

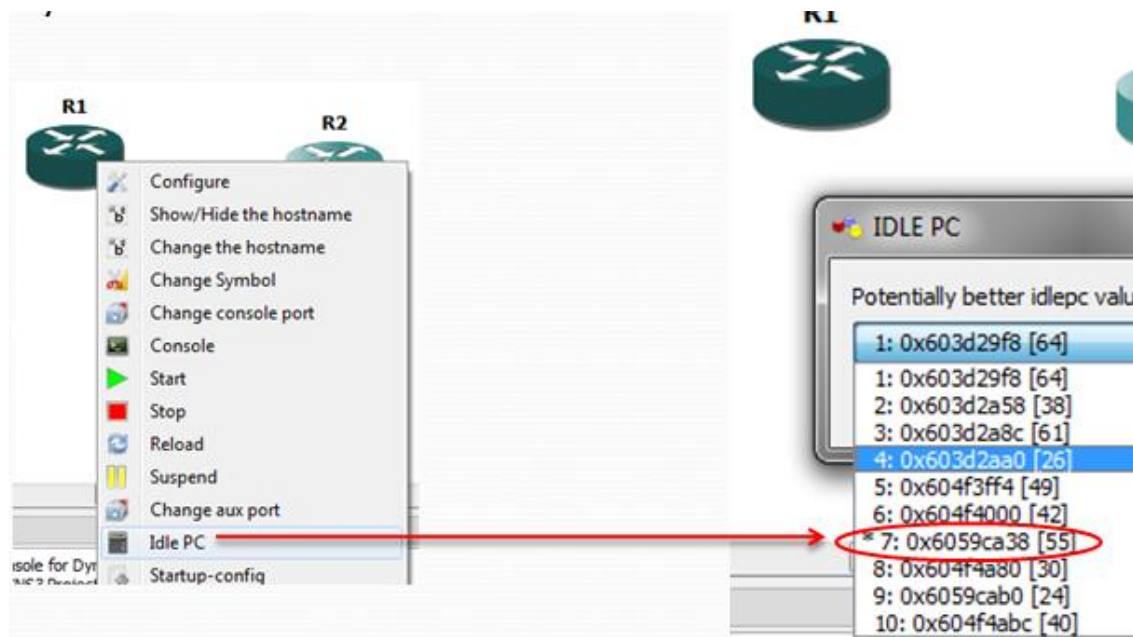


El uso de un router al iniciarse puede llegar a este punto o mas aun.

Como consideración si se desean utilizar varios router de forma simultanea, esto puede generar un enlentecimiento de nuestro ordenador.

Es necesario el uso de la opción "IDLE PC"

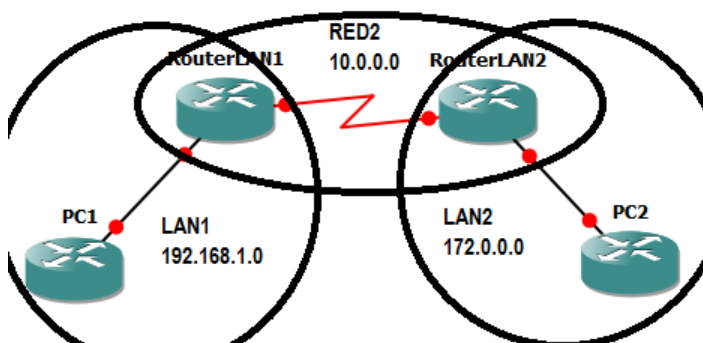
Paso 6: Para mejorar el rendimiento de nuestra PC es necesario recalcular el valor de IDLE PC en este caso GSN 3 señala con un * como mejor opción el valor 7.



Una vez realizado esto, debemos observar una disminución considerable en el uso del CPU. De no ser así, utilice otro valor de Idle PC.

Paso 7: Defina 3 redes junto con sus respectivas mascararas.

- ✓ La primera red será para la red que LAN que se encuentre bajo el RouterLAN1.
- ✓ La segunda red será la que opere entre los routers LAN1 y LAN2
- ✓ La tercera red operara debajo del RouterLAN2 y con PC2



En este caso utilizaremos 2 router como host de LAN.

Paso 8: Configure las terminales FastEthernet y Serial del Router conectado a LAN 1.

```
R1>enable
R1#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#hostname RED1
RED1(config)#int fa 0/0
RED1(config-if)#ip add 192.168.1.1 255.255.255.0
```

- a) No olvidemos el comando “no shutdown” pues de lo contrario no se activara el puerto a utilizar.
- b) Realice el mismo procedimiento para configurar el router perteneciente a la red LAN3.
- c) Utilice las direcciones IP sugeridas en la diapositiva anterior.

Paso 9: Configurando las interfaces seriales de los routers.

Utilice el comando exit para regresar al modo de configuración global.

Este comando permite configurar la terminal serial i/o

El clock rate establece la velocidad de transmisión de los datos.

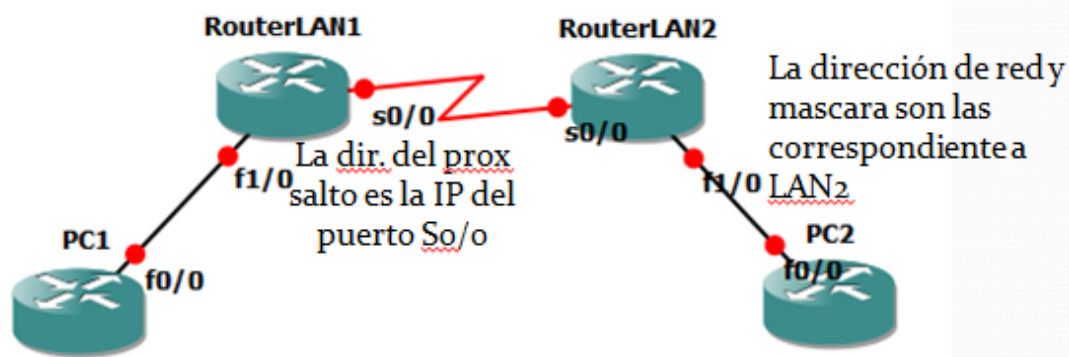
```
RED1(config)#int s1/0
RED1(config-if)#clockrate 128000
RED1(config-if)#ip add 10.0.0.1 255.255.255.0
RED1(config-if)#no shutdown
RED1(config-if)#
*Mar 1 00:09:07.503: %LINK-3-UPDOWN: Interface Serial1/0
RED1(config-if)#
*Mar 1 00:09:08.507: %LINEPROTO-5-UPDOWN: Line protocol
changed state to up
RED1(config-if)#
```

El clock rate debe ser colocado solamente en el extremo DCE de la conexión, pero al no saber cual es el DCE de la red, se utilizara en bos extremos.

Sin embargo para que los paquetes se transfieran de la red LAN1 hasta la red LAN2, es necesario cargar la siguiente línea de comandos.

IP route Direccion_de_la_red Mascara_de_la_red_remota Direccion_del_prox_salto

La siguiente imagen muestra una explicación breve sobre los elementos del comando anterior.



Paso 11: Configure los Routers PC1 y PC2 de acuerdo a la siguiente imagen.



```
Router>en
Router#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int f0/0
Router(config-if)#ip add 192.168.1.2 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
*Mar 1 00:02:11.719: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Mar 1 00:02:12.719: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
Router(config)#ip default-gateway 192.168.1.1
Router(config)#no ip routing
Router(config)#hostname PC1
```

Define el gateway del router

Deshabilita la función de routing.

Una vez configurados los equipos proceda a verificar las configuraciones, utilizando el comando ping entre PC1 y PC2.

VII. Preguntas de control

1. ¿Qué es GSN3?
2. ¿Cuál es la función de IDLE PC?
3. ¿Qué es un MicroCore de linux?
4. ¿Qué es un Qemu Host?
5. ¿Qué ventajas tiene GSN3 sobre Packet tracer?

I. Trabajo previo

- ✓ Investigar sobre GSN3.
- ✓ Leer sobre Dynamips y Dynagen.
- ✓ Descargue IOS de routers c3640.
- ✓ Descargue microcores de Linux para qemu host de GSN3



Laboratorio No. 12: Protocolo de conmutación por etiqueta MPLS

Curso	Capacitación en telefonía IP		
Modulo	Redes de Datos	Grupo	
Tipo Practica	<input type="checkbox"/> Laboratorio	<input type="checkbox"/> Simulación	
Unidad Temática			
No Alumnos por practica	1	Fecha	
Nombre del Profesor			
Nombre(s) del Alumno(s)			
Tiempo estimado	180 minutos	Vo. Bo. Del Docente	
Comentarios			

Objetivos de la práctica de laboratorio

I. Objetivo General

1. Desarrollar la configuración básica de una red MPLS.

II. Objetivos específicos

1. Mostrar los comandos para establecer el funcionamiento del protocolo LDP.
2. Configurar los protocolos BGP e iBMGP en router cisco 3600.
3. Establecer una red privada virtual utilizando MPLS.

III. Medios a utilizar

- Equipo de computo
- Programa simulador de redes GNS3.

IV. Introducción

El protocolo MPLS o conmutación de multiprotocolos por etiqueta, es una método que permite el reenvío de paquetes a través de una red utilizando la información contenida en etiquetas añadidas a los paquetes IP en el momento que estos entran a la red MPLS.

MPLS permite crear redes flexibles y escalables con un incremento en el desempeño y la estabilidad. Esto incluye aspectos como ingeniería de tráfico y soporte de redes virtuales privadas. También permite implementar calidad de servicio (QoS) con multiples clases de servicio (CoS).



En el enrutamiento tradicional los paquetes son reenviados de un enrutador a otro, cada enrutador hace una decisión de reenvío independiente por cada paquete y se realiza una clasificación dentro de una FEC basándose en prefijos y máscaras.

En MPLS, el paquete entra a la red inmediatamente y es asignado a una FEC, en análisis del encabezado ya no es hecho por los enrutadores subsecuentes. Todo el reenvío es hecho basado en etiquetas.

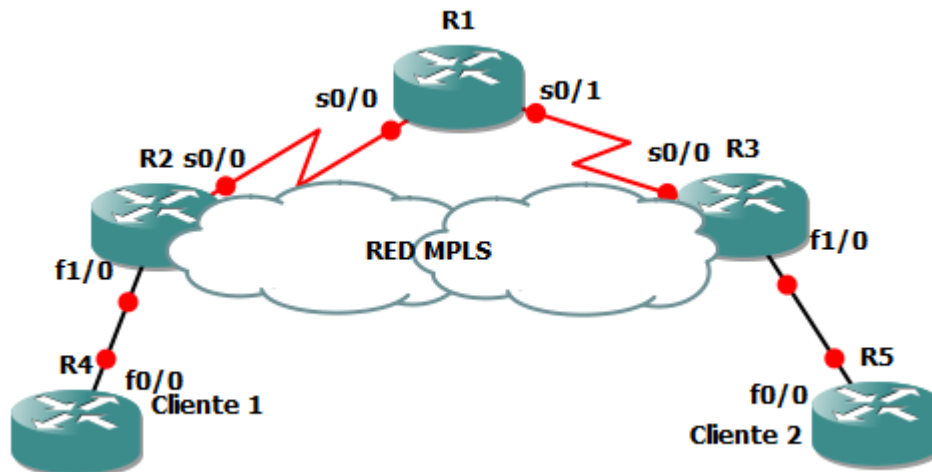
MPLS como se mencionó anteriormente soporta la creación de VPNs. A su vez, las redes MPLS poseen una gran escalabilidad al poder brindar este servicio a un gran número de clientes. Los servicios de valor agregados pueden implementarse en estas redes junto con un mejor aprovechamiento de la infraestructura ya existente.

V. Conocimientos previos

- Protocolos OSPF, BGP e iMBGP.
- Redes privadas virtuales
- Programación básica de interfaces seriales.
- Configuración de protocolo OSPF en redes IP
- Funcionamiento de redes MPLS.

VI. Procedimiento

Actividad 1. Configuración del escenario



Dispositivo	Puerto	Dirección IP	Mascara de red
R4	Fa 0/0	10.0.0.1	Clase C
R2	Fa 1/0	10.0.0.2	Clase C
R2	S 0/0	10.0.1.1	Clase C
R1	S 0/0	10.0.1.2	Clase C
R1	S 0/1	10.0.2.1	Clase C
R3	S 0/0	10.0.2.2	Clase C
R3	Fa 1/0	10.0.3.1	Clase C
R5	Fa 0/0	10.0.3.2	Clase C

Paso 1. Interconecte los dispositivos según muestra la figura anterior.

Los router a utilizar son los C3600. Recuerde que los enlaces entre los router R1, R2 y R3 son seriales. Y al momento de conectarlos debe utilizar el cable DCE iniciado en R2 para que se reconozca que este será el DCE.

En el caso de las interfaces seriales deberá agregar los módulos seriales antes de conectarlos.

Paso 2. Proceda a asignar las direcciones IP a las terminales de los dispositivos, según se muestran en la tabla de referencia.



Paso 3. Configure las terminales DCE con un clock rate de 64000.

Paso 4. Verifique que las terminales están conectadas y existe comunicación entre ellas enviando mensajes ICMP entre los puntos conectados directamente.

Ingresa a la línea de comando de cada router y utilice el comando ping. En este punto la red solo debe ser capaz de enviar y recibir mensajes ICMP entre nodos adyacentes.

Actividad 2. Configuración de la interfaz loopback

La interfaz loopback sirve como un identificador para el router en que se configura.

Hacemos énfasis en configurarle porque es necesaria para la configuración del protocolo OSPF y BGP que se configuraran más adelante, pues se asocia la interfaz loopback a procesos en OSPF y BGP.

Las sesiones OSPF o BGP requieren de la existencia de una interfaz, en caso de asociarlo a una interfaz física, se corre el riesgo que esta se dane y se pierda la conexión. Por ende se prefiere asociar los procesos a una interfaz virtual.

Paso 1. Para configurarle se utilizan los comandos:

R1# configure terminal

R1(config)# interface loopback 0

R1(config)# ip address 192.168.1.1 255.255.255.0



Solamente los router R1, R2 y R3 se configuraran con las interfaces loopback. Las interfaces pueden denotarse por cualquier número; en este caso, le llamamos 0. Las direcciones IP de las interfaces loopback deben ser distintas entre los router pero deben pertenecer todas a la misma red. Es decir, a la red 192.168.1.0.

Paso 2. Realice el proceso del paso 1 para los router R2 y R3, asignados diferentes direcciones IP.

Paso 3. Verificación de las interfaces loopback

Verifique que las interfaces loopback se han configurado correctamente en cada router utilizando el comando

R1# show ip interface brief

Actividad 3. Configuración OSPF

Paso 1. Para configurar el protocolo OSPF seguiremos el procedimiento desarrollado en el laboratorio 9.

Los comandos son:

R1# configure terminal

R1(config)# router ospf 1

R1(config – router)# network 10.0.0.0 0.0.0.255 area 1

R1(config – router)# network 10.0.1.0 0.0.0.255 area 0

R1(config –router)#^Z



En este caso, se han definido 3 áreas OSPF. Las área 1 y 2 corresponden a las secciones fuera de la red MPLS y el área 0 es el backbone de MPLS.

Paso 2. Realice el mismo procedimiento para los router R2 y R3.

Paso 3. En el caso de los routers R4 y R5 que pertenecen a los clientes 1 y 2, es necesario habilitar un comando para que este pueda establecer conexión con redes que no estén directamente conectadas a él.

R4#configure terminal

R4(config)# ip route 0.0.0.0 0.0.0.0 10.0.0.2

En el caso del router R5 seria:

R5# configure terminal

R5(config)# ip route 0.0.0.0 0.0.0.0 10.0.3.1

Paso 4. Revise que la configuracion de del protocolo OSPF es correcta a traves de los comandos:

R1# s hip ospf interface

R1# s hip opsf neighbors

Paso 5. Verifique que existe conectividad entre los router no adyacentes enviando mensajes ICMP entre los routers no adyacentes de la red MPLS y finalmente entre las router R4 y R5.

Actividad 4. Configuración del protocolo BGP



Para poder utilizar el protocolo MPLS en la red de área 0 es necesario con establecer un enmallado total entre los router pertenecientes a esta red. Realmente el uso de BGP en estas redes no es del todo necesario, ya que se puede implementar solamente utilizando el protocolos OSPF de IGP.

El objetivo de configurar BGP es para hacer uso de este protocolo al momento de configurar las redes privadas virtuales en la red MPLS.

Paso 1. Primero debemos establecer el enrutamiento BGP en la red de área 0. Para ello utilizamos la siguiente secuencia de comandos:

***R1# configure terminal
R1(config)# router bgp 65000***

En este caso 65000 representa el número de proceso bgp en el router R1. Se establece este valor porque es el usado en entornos de prueba.

Paso 2. Para cada pareja de routers adyacentes en la red MPLS es decir R2 con R1 y R1 con R3 es necesario especificar en uno de ellos cual es el router vecino y le indicamos que debe actualizar la tabla de encaminamiento a través de la interfaz loopback configurada anteriormente.

Configure al router vecino con la siguiente línea de comandos:

***R2#config terminal
R2(config)#router bgp 65000
R2(config –router)# neighbor <dir IP de la interfaz del router al que se conecta directamente> remote as < proceso bgp>
R2(config –router0# neighbor <dir Ip de la interfaz del router al que se conecta directamente> update-source loopback <número de la interfaz>***



La dir IP del router vecino en este caso sería 10.0.1.2 y el número de proceso es siempre 65000.

En el caso de que los router no estén directamente conectados, la dirección IP que hay que indicar es la de la interfaz de loopback del router remoto para que establezca relaciones de vecindad. Es decir:

R2(config-router)#neighbor <dir Ip de int loopback de R3> remote as 65000

En el router remoto es necesario especificar al router vecino con la interfaz de loopback que se ha configurado para que sirva de medio para actualizar el enrutamiento.

Paso 3. Verifique el proceso de configuración del protocolo BGP.

Utilice el comando ***sh ip bgp neighbor*** este comando le permitirá ver los router que mantienen una relación de vecindad con el router en el que se ejecuta el comando, así como la información relativa a esa relación.

Para verificar el estado de vecindad de los routers utilice el comando ***sh ip bgp summary***.

Actividad 4. Configuración básica de MPLS.

El escenario para establecer el protocolo MPLS ya está listo, ahora es necesario iniciar el protocolo de distribución de etiquetas en las distintas interfaces en las que se desea se transmita a través de etiquetas.



Paso 1. Configure el reenvío express de cisco en todos los router que tienen funcionalidad PE y P. CEF es el conjunto de funcionalidades que reúnen los equipos CISCO para poder trabajar en un entorno MPLS en otras funciones.

Los comandos a utilizar son:

R1# configure terminal

R1(config)# ip cef

Para comprobar que el CEF ha sido activado en el router es necesario utilizar el comando **sh ip cef summary**. Si está activado nos mostrara una tabla sobre los comandos hábiles en el router. Algo importante es la versión de esta tabla, algunas tablas pueden activarse pero si la versión no es tan reciente puede que el router no reconozca algunos comandos de MPLS.

Paso 2. Este mismo proceso se debe llevar a cabo en los router R2 y R3.

Paso 3. Activación del protocolo de distribución de etiquetas LDP.

En esta parte designaremos que interfaces redirigen mediante el protocolo MPLS. Note que solamente las interfaces seriales de los routers utilizaran MPLS.

Los comandos a utilizar son:

R1 (config)# interface s0/0

R1 (config – if)# mpls ip

R1 (config – if)# mpls label protocol ldp

R1 (config – if)# exit

R1 (config)# interface s0/1

R1 (config – if)# mpls ip

R1 (config – if)# mpls label protocol ldp

Paso 4. Realice el mismo proceso para las interfaces seriales de los router R2 y R3.



Paso 5. Verifique que los parámetros e interfaces mpls han sido configurados correctamente, usando los comandos:

R1# show mpls interfaces

R1# show mpls ldp parameters

Actividad 5. Configuración de VPN sobre MPLS

Paso 1. Se configuran el enrutamiento y reenvío asociado a la VPN en los routers a utilizar. Estas se denominan VRF, incluyen las tablas de envío y encaminamiento de los sitios pertenecientes a una VPN.

Para configurarle se necesitan algunos parámetros como:

- Señalador de rutas (RD) que permite identificar de forma única un prefijo de VPN –IPv4.
- Route-Target (RT) que identifica los routers que deben recibir la ruta.

Para dar a entender estos parámetros a los router se usan los siguientes comandos:

R1# configure terminal

R1(config)# ip vrf “nombre de la vrf”

R1(config –vrf)#rd “valor del rd”

R1(config – vrf)#route-target export “valor que tiene que exportar”

R1(config – vrf)#route-target import “valor que tiene que importar”

En nuestro caso, por la naturaleza de la configuración utilizada donde se muestra que todo pasa a través del router R1 se considera el caso de una topología hub&spoke. El router R1 funciona como hub y los router R2 y R3 funcionan como dispositivos spoke.



Los comandos a utilizar en R1 son:

R1# configure terminal

R1(config)# ip vrf “nombre de la vrf”

R1(config –vrf)#rd “valor del rd”

R1(config – vrf)#route-target export “valor que tiene que exportar”

R1(config – vrf)#route-target import “valor que tiene que importar”

En los dispositivos spoke son:

R1# configure terminal

R1(config)# ip vrf “nombre de la vrf”

R1(config –vrf)#rd “valor del rd”

R1(config – vrf)#route-target export “valor que tiene que importar el hub”

R1(config – vrf)#route-target import “valor que tiene que exportar el hub”

Paso 2. Ahora configuraremos las interfaces de los PE que se encuentran conectadas a los CE. Es decir, conectadas a los routers R4 y R5.

Los comandos para redirigir los datos a travez de la VPN son:

R2# configure terminal

R2(config)# interface Fa 1/0

R2(config –if)# ip vrf forwarding <nombre de la vrf>

Paso 3. Asignamos la dirección IP a la interfaz donde se acaba de configurar el reenvió dentro de la VPN, ya que pierde el direccionamiento de dicha interfaz.



Al ejecutar el reenvío de vrf se pierde la configuración IP por lo que es necesario volver a configurarla.

R2(config)# int fa 1/0

R2(config – if)# ip address 10.0.0.2 255.255.255.0

Paso 4. Realice el mismo proceso para la interfaz Fa del router R3.

Paso 5. Ahora configuraremos el enrutamiento dinamico en la VRF creada:

Es necesario crear un nuevo proceso OSPF dedicado al enrutamiento dentro de la VRF. Para ello:

R2(config)# router ospf <id del proceso> vrf <nombre vrf>

Y el área en la que se encuentran las interfaces pertenecientes a la VPN.

R2(config –router)# network 10.0.1.0 0.0.0.255 área 0

Paso 6. Repetir este proceso para los router R1 y R2

Para que los prefijos que se han aprendido circulen entre los equipos del proveedor de servicio es necesario configurar el protocolo iMBGP.

R2(Config)# router bgp <número del proceso bgp asignado inicialmente>

Si no lo recuerda utilice el comando “sh ip bgp summary” para saber el número de proceso bgp activo.

R2(config –router)# address –family vpnv4

R2(config – router – af)# neighbor <dir IP del vecino iBGP> active



R2(config – router – af)# neighbor <dir lp del vecino iBGP> send-community both

Paso 7. Debe realizar este mismo proceso en los router R2 y R3.

Paso 8. Una vez que las sesiones iMBGP han sido establecidas solo falta propagar lo prefijos locales al resto de equipos PE para que estos sepan reenviar el paquete hasta dicho prefijo. Para esto es necesario redistribuir OSPF en el iMBGP.

R1# configure terminal

R1(config)# router bgp < número del proceso bgp que este configurado>

R1(config – router)# address-family ipv4 vrf <nombre del vrf>

R1(config –router – af)# redistribute ospf <identificador del proceso ospf del paso 5 > vrf <nombre del vrf>

“Haga el mismo proceso para los routers R2 y R3”

Paso 9. Verifique que las configuraciones están correctas utilizando el comando ping o traceroute.

VII. Preguntas de control

1. ¿Para qué sirve la interfaz loopback?
2. ¿Cuál es la función del protocolo BGP?
3. ¿Qué es CEF?
4. ¿Qué es VRF?
5. ¿Para qué sirve el VRF?
6. ¿Qué es una topología Hub&Spoke?



VIII. Trabajo previo

- ✓ Investigar sobre el funcionamiento de protocolos MPLS
- ✓ Procesos BGP
- ✓ Protocolo BGP e iMBGP
- ✓ Interfaces Loopback
- ✓ Dispositivos PE y CE en MPLS
- ✓ Implementación de VPNs en MPLS



Guías Prácticas del Módulo III: Telefonía IP





Laboratorio No. 1: Configuración de Hipath 3000 via DTMF *

Modulo	Telefonía IP		
Tipo Práctica	<input type="checkbox"/> Laboratorio <input type="checkbox"/> Simulación		
Unidad Temática			
No Alumnos por práctica	2	Fecha	
Nombre del Profesor			
Nombre(s) de Alumno(s)			
Tiempo estimado		Vo. Bo. Del Profesor	
Comentarios			

Objetivos de la práctica de laboratorio

I. Objetivo general

1. Configurar la PBX Hipath 3000 con los teléfonos Siemens Optipoint 500 Standard vía DTMF.

II. Objetivos específicos

1. Inicializar Teléfonos Siemens Optipoint 500 Standard para su utilización.
2. Programar servicios básicos de uso habitual en los Teléfonos Siemens Optipoint 500 Standard.

III. Medios a utilizar

- PBX Hipath 3000
- Teléfonos Siemens Optipoint 500 Standard

IV. Introducción

Muchas veces es necesario enviar dígitos a través de la línea telefónica tanto para marcar como en medio de una conversación. Con esta finalidad se pensaron los DTMFs.

DTMF es un acrónimo de Dual-Tone Multi-Frequency. Es decir que cada DTMF es en realidad dos tonos mezclados enviados simultáneamente por la línea telefónica: uno por columna y otro por fila en la que esté la tecla, que la central



descodifica a través de filtros especiales, detectando instantáneamente que dígito se marcó. Esto se hace así para disminuir los errores.

A continuación una tabla ilustrando los pares de frecuencias para cada dígito:

	1209 Hz	1336 Hz	1477 Hz	1633 Hz
697 Hz	1	2	3	A
770 Hz	4	5	6	B
852 Hz	7	8	9	C
941 Hz	*	0	#	D

En esta práctica se realizan configuraciones básicas tales como el cambio de idioma, inicialización de los teléfonos, modificación de fecha y hora a través de teléfonos Siemens Optipoint 500 Standard todo vía DTMF.

También se programan servicios básicos de uso habitual en los Teléfonos Siemens Optipoint 500 Standard como el servicio Hotline, No molestar, Desvió de llamadas, Programación de teclas y la función de Conferencia.

Como se mencionó anteriormente el teléfono a utilizar es el Optipoint 500 Standard de Siemens, cuyo panel de operación se muestra en la figura 1. Se trata de un diagrama bien detallado de los elementos del teléfono.



Fig. 9 Teléfono Optipoint 500 Standard

A partir de aquí se harán todas las configuraciones necesarias.

V. Conocimientos previos

- Diagrama del hardware de la PBX Hipath 3000.
- Diagrama del teléfono Siemens Optipoint 500 Standard
- Marcación por tonos o DTMF.
- Central Privada o PBX (Private Branch eXchange).
- Servicios que brindan las PBX.

VI. Procedimiento

El escenario a implantarse se muestra en la figura 2. Aquí se presentan los medios a utilizar como son la centralita Hipath 3000 modelo de pared 3550 y el Teléfono Digital Siemens Optipoint 500 Standard:

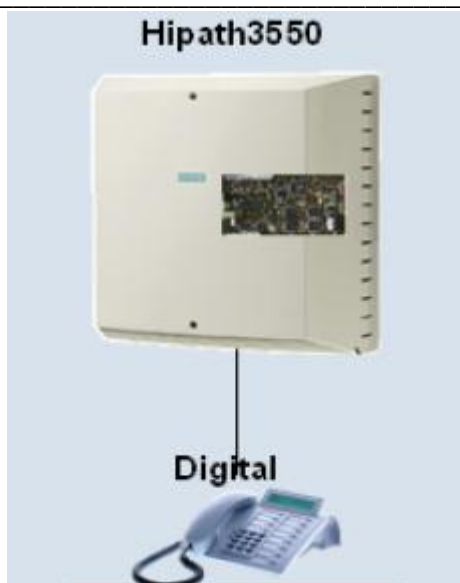


Fig. 10 Escenario del laboratorio

Actividad 1: Inicialización del Teléfono

1. Conecte la centralita Hipath 3000 al suministro eléctrico y oprima el switch de encendido/apagado.
2. Espere unos minutos hasta que la centralita pueda cargar toda la programación contenida en su KDS (base de datos de la central). Inmediatamente de esto los teléfonos se reinician y los LEDs al lado de las Teclas de función empiezan a parpadear.
3. Destape con sumo cuidado la carcasa de la centralita Hipath 3000 y seguido de esto oprima el botón reset ubicado en la tarjeta módulo de mando Central Board with Coldfire Com (CBCC) durante 5 segundos, que se muestra en la figura 3.

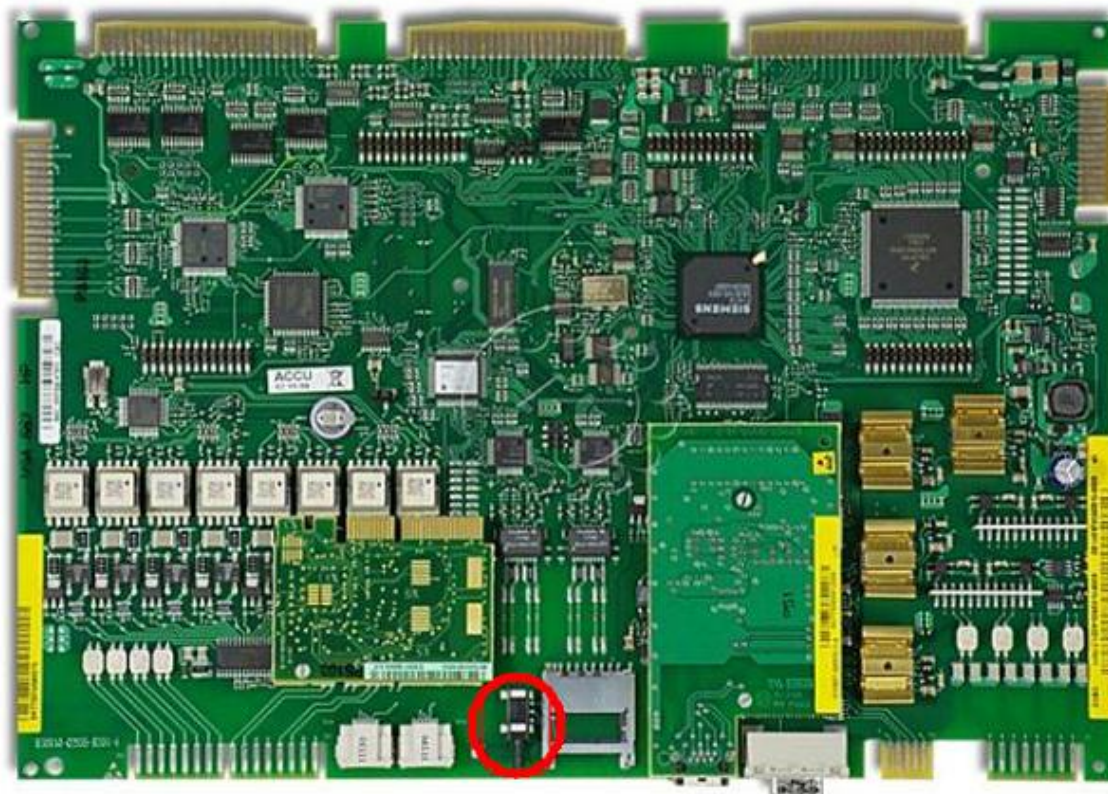


Fig. 11 Tarjeta Módulo de Mando CBCC

4. Este paso se realiza con el objetivo de borrar la programación existente en la centralita Hipath 3000 y que esta vuelva al estado de suministro. Al igual que el paso anterior deberá esperar que los Teléfonos vuelvan a encender.

Actividad 2: Cambio de idioma

1. Diríjase al Teléfono Optipoint 500 Standard. En parte superior izquierda del display se logra apreciar la hora y en la parte inferior el número de extensión correspondiente. En la parte superior derecha aparece la fecha y en la parte inferior el nombre de la centralita Hipath acompañado de una viñeta que se utiliza para desplegar más opciones, esto con la tecla direccional derecha.

Nota: Observe en el display que el idioma por defecto es el alemán, por ser propietario de Siemens.



-
2. Presione *48 y desplácese con las flechas direccionales al idioma de preferencia o simplemente presione 15 que corresponde al idioma español y posteriormente presione Confirmar.

Actividad 3: Inicialización del país

1. Introduzca *95 para entrar a la administración del sistema. Se le pedirá un nombre de usuario y una contraseña. El nombre de usuario por defecto es 31994 de igual forma que la contraseña.
2. Ingrese dos veces más la confirmación de la contraseña.
3. Busque la opción 29 (Datos del Sistema) y seleccione el campo número 5 (Inicialización país).
4. Seleccione password variable. Aquí saldrán varios países y contiene por defecto el país Alemania, seleccione modificar y elija Internacional (opción 21) luego confirme los cambios.
5. Espere la reiniciación de los Teléfonos.
6. Cambie de nuevo el idioma.

Todas las opciones que aparecen en el menú Administración del Sistema se encuentran en la sección de anexos de la guía.

Actividad 4: Ajuste de hora y fecha

1. Entre a la Administración del Sistema con *95 con nombre de usuario y contraseña 31994.
2. Seleccione la opción Indicación display (o bien presione 19) y escoja la opción 13 (Ajuste de la hora).
3. En el display aparecerá el formato de la hora, siga dicho formato y modifíquelo.
4. Vuelva al menú anterior presionando F7 y elija la opción 14 (Ajuste de la fecha) siga el formato que aparece ahí y modifíquelo.



Actividad 5: Programación de servicios

Actividad 5.1: Hotline

1. Active el modo de programación *95 con nombre de usuario y contraseña 31994.
2. Seleccione la opción 61 que es hotline.
3. Entre en destino hotline aparecen varias direcciones hotline que van desde hotline 1 hasta hotline 6.
4. Elija la dirección hotline 1 y luego presione modificar.
5. Digite la extensión de destino que esté disponible a la cual se desea llamar y luego presione confirmar.
6. Presione F2 para continuar. A continuación aparece el menú de extensión hotline.
7. Seleccione modo hotline y luego presione modificar para activar el servicio. Todas las extensiones por defecto vienen en “no”. Seleccione 1=sí en la extensión que desee esté activo este servicio y luego confirmar.
8. Presione F2 para continuar.
9. Seleccione asignación hotline y elija la extensión en la que desee esté activo este servicio.
10. Elija hotline 1 que tiene la extensión a la cual desea marcar, introduciendo el número 1 en modificar y luego confirmar.
11. Presione F2 para continuar.
12. Levante el teléfono con la asignación hotline para comprobar que la llamada se redirige a la extensión seleccionada.

Actividad 5.2: No molestar

1. Active el modo de programación *95 con nombre de usuario y contraseña 31994.



2. Seleccione la opción 14 la cual es extensiones.
3. Elija el número 20 es decir No molestar.
4. En No molestar aparecen todas las extensiones existentes dentro del sistema, en cada extensión sale indicado si la función se encuentra activa o no.
5. Para cada extensión aparece el siguiente menú:
 - + = Hojear
 - * = Modificar
 - # = Marcar extensión
 - F2= Continuar
 - F7= Volver atrás
6. Se elige la extensión en la cual se quiere activar el servicio, se presiona modificar 0 = No y 1= Si, se presiona 1 y luego continuar, de esta manera el servicio queda activo en la extensión deseada.

Actividad 5.3: Desvío de llamadas

1. Presione *1 para entrar al menú de desvío de llamadas.
2. Seleccione del menú sólo llamadas internas.
3. A continuación nos pide la extensión a la cual se va a desviar la llamada. Digite una extensión disponible y seleccione almacenar.
4. Para desactivar el modo de desvío de llamadas haga click en la viñeta que aparece en la parte derecha y seleccione desvío no.

Actividad 5.4: Programación de teclas

1. Ingrese *91 y presione la tecla de funciones que se desea programar, una vez elegida la tecla a modificar, se listan en el display una serie de opciones dentro de las cuales se puede elegir la función que se quiere para esa tecla. Desplácese con las teclas + y – para observar todas las funciones disponibles.



2. Seleccione una de las opciones del menú para que esa función quede programada en la tecla elegida, de esta manera la tecla seleccionada se convierte en un acceso rápido a ese servicio.
3. Presione la tecla que se programó para asegurarse que la función asignada funcione correctamente.

Actividad 6: Conferencia

1. Marque la extensión con la cual se desea comunicar.
2. Cuando la extensión a la que se llama levanta la extensión, aparecerán varias opciones en el display. Seleccione Iniciar conferencia.
3. A continuación se pedirá el otro número con el cual se desea establecer la conferencia. Digite dicho número.
4. Cuando conteste la tercera extensión con el cual se desea establecer la conferencia, aparecerá en el display Conferencia? A continuación pulse confirmar. De esta manera ya se tiene entablada la conferencia.

Actividad 7: Asignación

1. Seleccione un servicio de la tabla mostrada en los anexos, sin incluir los servicios mostrados en la actividad 5.
2. Programe dicho servicio.
3. Elabore el procedimiento utilizado en la programación tal como se muestra en la actividad 5.

VII. Preguntas de control

1. ¿Cuál es el clave que se utiliza para entrar a administración del sistema?
2. ¿Por qué cree usted que el idioma es ingles cuando se elige el país como internacional?
3. ¿Qué pasa si el botón reset sólo se presiona durante dos segundos?



4. Mencione las dos maneras vía DTMF que existen para modificar la hora y la fecha.

VIII. Bibliografía

Siemens Communications, Instrucciones de manejo de los teléfonos optiPoint 500 economy, optiPoint 500 basic, optiPoint 500 standard y optiPoint 500 advance en el HiPath 500 y HiPath 3000 / 5000. © Siemens AG 2006. <http://www.telprom-maresme.com/linked/tel.%20optipoint%20500.pdf>

IX. Anexos

Opciones del menú Administración del Sistema

11-Tarificación	28-Abrir KDS
12-Marcación abreviada común	29-Datos del sistema
13-Código proyecto	30-Tele programación
14-Extensiones	31-Menú UCD
15-Control marcación	32-Equipo buscapersonas
16-Llamadas entrantes	33-Operadora
17-Red externa	34-DISA
18-Tráfico interno	35-Búsqueda de rutas
19-Indicación display	36-Inalámbrico
20-Parámetros RDSI	37-Seguridad
21-Líneas A/B	52-Ajuste de la hora
22-Parámetros del sistema	53-Ajuste de la fecha
23-Código selección	58-Selección del idioma
24-Portero automático	61-Hotline
25-Equipo de anuncios	62-Código de tele programación
26-Contactos	63-Clave inalámbrico
27-Sensores	F7= volver atrás

Para obtener una lista completa de todos los servicios que vienen precedidos de asterisco o numeral presione la tecla de función menú servicio que aparece en la



figura 1. A continuación se enlistan cada uno de los servicios que aparecen al presionar esa tecla:

*0-Recuperar llamada	*68-Mandar mensajes
*1-Desvío	*69-Texto
*2-Comunicación alternativa	*7-Numero abreviado
*41-Numero MSN	*80-Interfono
*42-Código TDS	*81-Sin timbre adicional
*43-Liberar línea	*82-Almacenar numero
*44-Servicio nocturno	*86-Supresión numero
*46-Programar cita	*87-aviso llamada sin tono
*47-Numero DISA	*91-Programación tecla
*48-Selección idioma	*92-Grabar numero
*491-Timbre externo	*93-Cambiar clave candado
*494-Aplicación	*940-Chequeo telefónico
*495-Desvío CFNR a	*942-Clave
*508-Teléfono Temporal	*943-Candado central
*51-Flash por línea	*96-Respuesta a interfono
*52-Micrófono	*98-Llamada silenciosa
*53-Emitir tonos	*993-Cambiar código acceso
*54-Voicemail	*994- Índice rellamada
*55-Aceptar llamada	#0-Desactivar servicio
*58-Lista devoluciones	#56-Desaparcar llamada
*59-Captura extensión	#68-Información enviada
*60-Código cuenta	#82-Lista llamadas
*62-Intercalación	#86-Transmitir numero
*63-Recupera línea	#943-Inicializar candado
*65-Consultar gasto	#96-Respuesta a interfono
*66-Candado	F7= volver atrás



Laboratorio No. 2: Configuración de Hipath 3000 via software *

Modulo	Redes de Telefonía		
Tipo Práctica	<input type="checkbox"/> Laboratorio <input type="checkbox"/> Simulación		
Unidad Temática			
No Alumnos por práctica	2	Fecha	
Nombre del Profesor			
Nombre(s) de Alumno(s)			
Tiempo estimado		Vo. Bo. Del Profesor	
Comentarios			

Objetivos de la práctica de laboratorio

I. Objetivo general

1. Programar servicios brindados por la PBX HiPath 3000 mediante el software Hipath 3000 Manager E V8.

II. Objetivos específicos

1. Ajustar los parámetros de comunicación del software Manager E V8.
2. Configurar extensiones telefónicas.
3. Programar teclas en los teléfonos Siemens Optipoint 500 Standard
4. Asignar servicio Hotline en la Hipath 3000
5. Configurar teléfonos Siemens Optipoint 500 Standard vía online

III. Medios a utilizar

- PBX Hipath 3000
- Teléfonos Siemens Optipoint 500 Standard
- Equipo de cómputo
- Cable conexión doble 2 x RS232 Sub-D 9 pins hembra

IV. Introducción



Hipath 3000 Manager E es el programa de administración para el sistema de comunicación HiPath 3000. Este software se instala en el ordenador de forma que facilita la administración de la central telefónica.

A través del Hipath 3000 Manager E se realizan las mismas configuraciones que en laboratorio DTMF tales como cambio de idioma, de país y modificación de fecha y hora a través del modo Online del software Manager E V8.0.

El modo Online permite al usuario hacer configuraciones en la central a través del software simulando un teléfono como en el laboratorio DTMF en tiempo real. El procedimiento y los códigos son los mismos que en laboratorio DTMF.

La principal ventaja acerca del Manager E es que usted puede descargar un archivo KDS (base de datos) y modificarlo tantas veces como quiera sin cambiar el sistema en caliente, o sea mientras esté trabajando.

Se debe descargar una KDS antes de hacer cualquier trabajo, o bien cargar una KDS guardada, hacer los cambios y luego realizar la transferencia de nuevo al sistema. Si algo sale mal sólo puede cargar la KDS original que se tenía guardada.

En este laboratorio se le enseña al estudiante como utilizar el software antes mencionado en sus aspectos básicos, tales como la transferencia de la información hacia la central y como guardar los cambios efectuados.

La diferencia entre este laboratorio y el laboratorio DTMF es que a través del software Hipath 3000 Manager E se tiene un interfaz más agradable para la persona que está realizando la configuración por medio del software.

V. Conocimientos previos

- Diagrama del hardware de la PBX Hipath 3000.
- Diagrama del Teléfono Siemens Optipoint 500 Standard
- Marcación por tonos o DTMF.
- Central Privada o PBX (Private Branch eXchange).
- Servicios que brindan las PBX.
- Laboratorio 1: Configuración de Teléfonos Siemens vía DTMF.

VI. Procedimiento

El escenario a implantarse se muestra en la Figura 1. Aquí se presentan los medios a utilizar como son la centralita Hipath 3000 modelo de pared 3550 y el Teléfono Digital Siemens Optipoint 500 Standard:

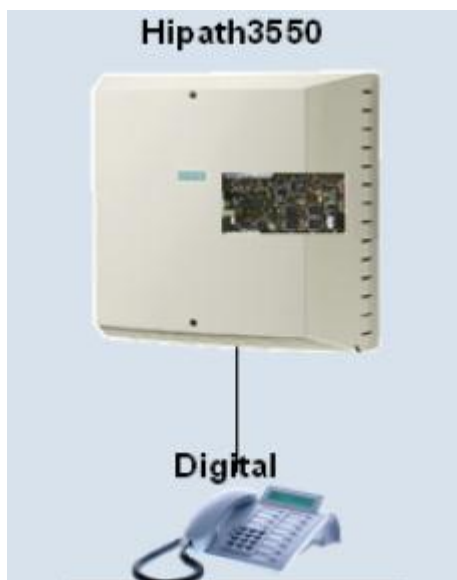


Fig. 1 Escenario del laboratorio

Actividad 1: Inicialización de la central

1. Siga el procedimiento descrito en la actividad 1 del laboratorio de DTMF.

Actividad 2: Configuración del Software

1. Conecte la Hipath 3000 al puerto COM de la computadora, si no se dispone de un puerto COM se puede utilizar un adaptador de USB a Serial RS-232.

2. Entre al programa Hipath 3000 Manager instalado en la PC. En seguida el software le pedirá un nombre de usuario y una contraseña. El nombre de usuario por defecto es 31994 de igual forma la contraseña.
3. El programa trae como idioma por defecto el inglés, para cambiar el idioma: Hacer click en Option, luego program option, en general busque select language y elija spanish. Espere que el idioma cambie.

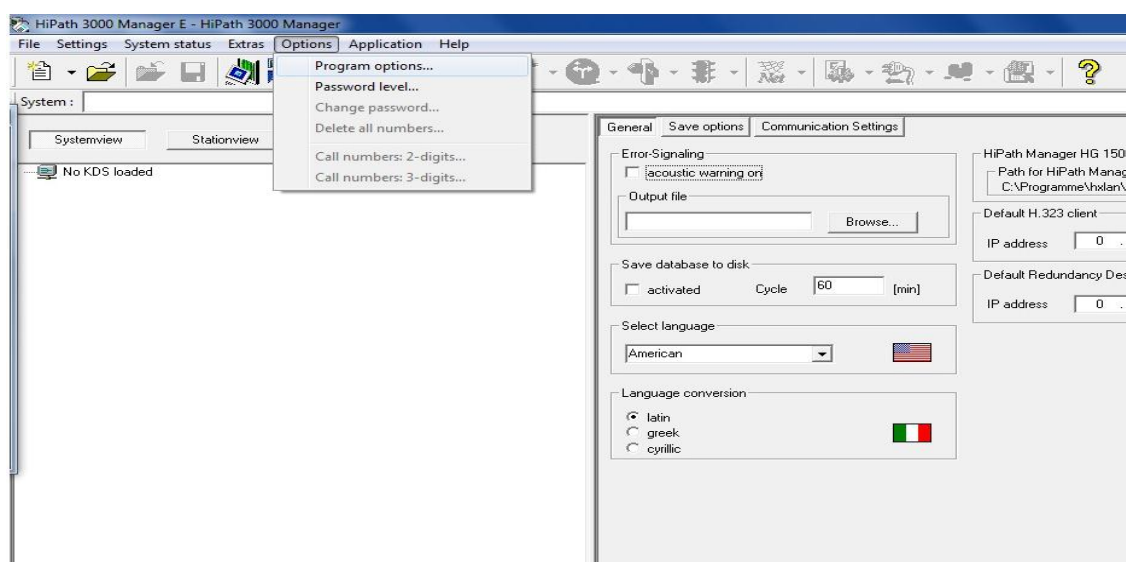


Fig. 2 Cambio de idioma

4. Seleccione opciones, opciones de programa.
5. Elija comunicación.
6. En la pestaña de comunicación se cambian algunos parámetros del sistema como el módem que se desea utilizar, el tipo de cable y la velocidad de transmisión, se elige Creatix Joe 33.6, v.24 y 9600 respectivamente para la conexión del servicio de PC.
7. El puerto se selecciona en base a lo que está instalado en la PC, por lo general se selecciona el COM1, pero en caso de que se utilice dicho adaptador se selecciona el puerto COM12 o COM13. Si no se cuenta con estos puertos es necesario usar un adaptador de USB a Serial RS-232.

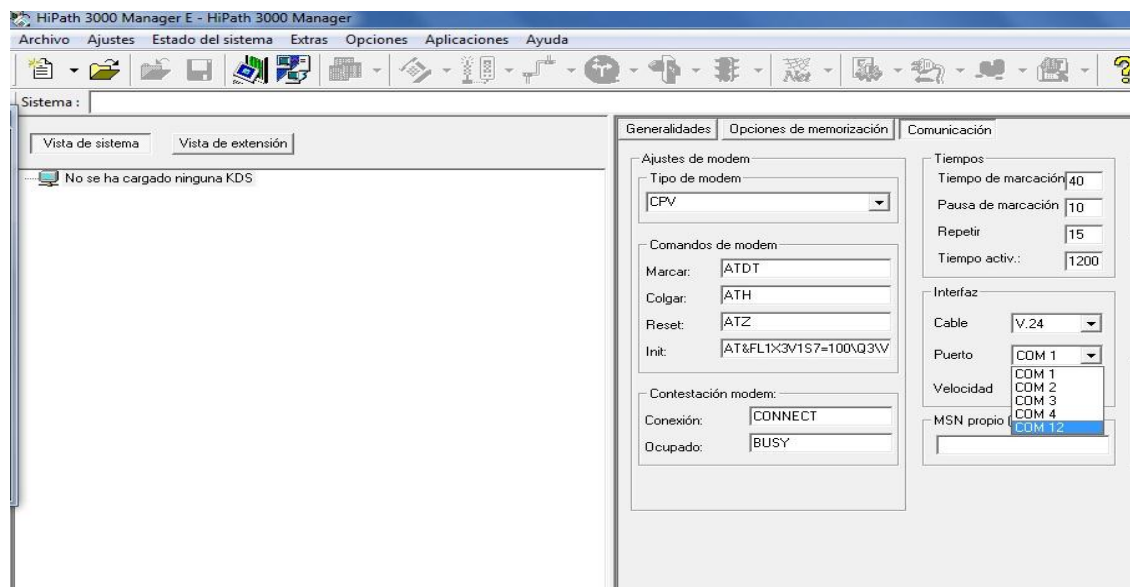



Fig. 3 Comunicación

Actividad 3: Cargar base de datos del sistema

1. De click en el icono transferir  de la barra de herramientas del sistema.
2. Ajuste la clave del sistema. Esto solo se hace una sola vez.
3. Seleccione Seguridad.
4. Aquí le pedirán la nueva clave y la confirmación de esta, en este caso ponga la clave por defecto 31994.
5. Confirme los cambios
6. Una vez que se guardó la clave, dentro del icono Transferir en la pestaña Comunicación seleccione modo directo.
7. Seleccione Leer/Escribir KDS.
8. Escoja la opción IVM download, de esta forma se descarga el Integrated Voice Mail (Correo de voz integrado) el cual es el módulo de extensión.
9. De click en Sistema a PC, para descargar los datos de la PBX.

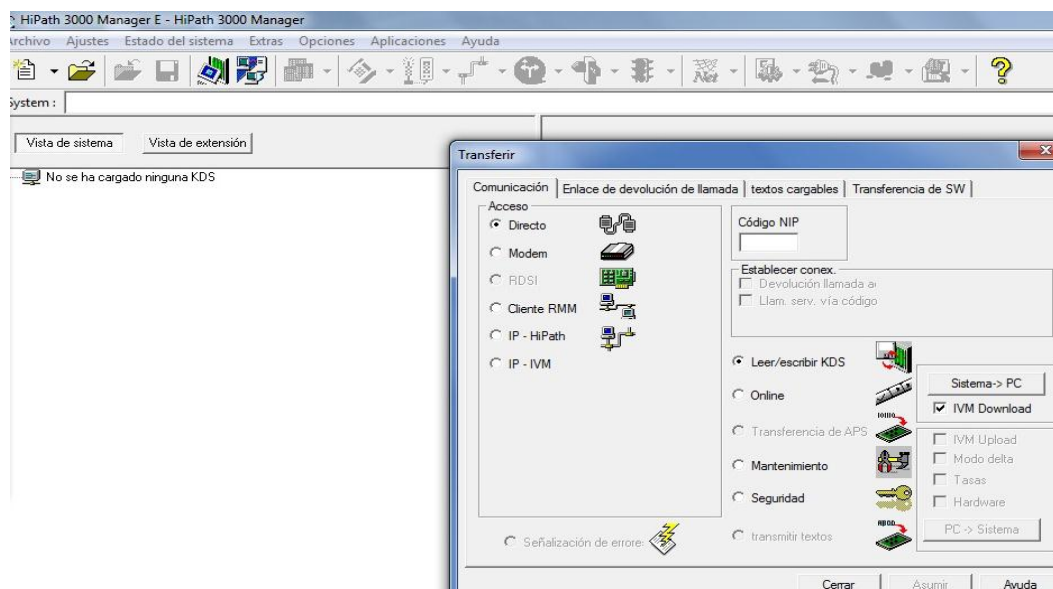


Fig. 4 Leer/Escribir KDS

10. Aparecerá una ventana que dice Información de Registro y luego aparece una ventana que muestra la transacción de datos de la PBX a la PC

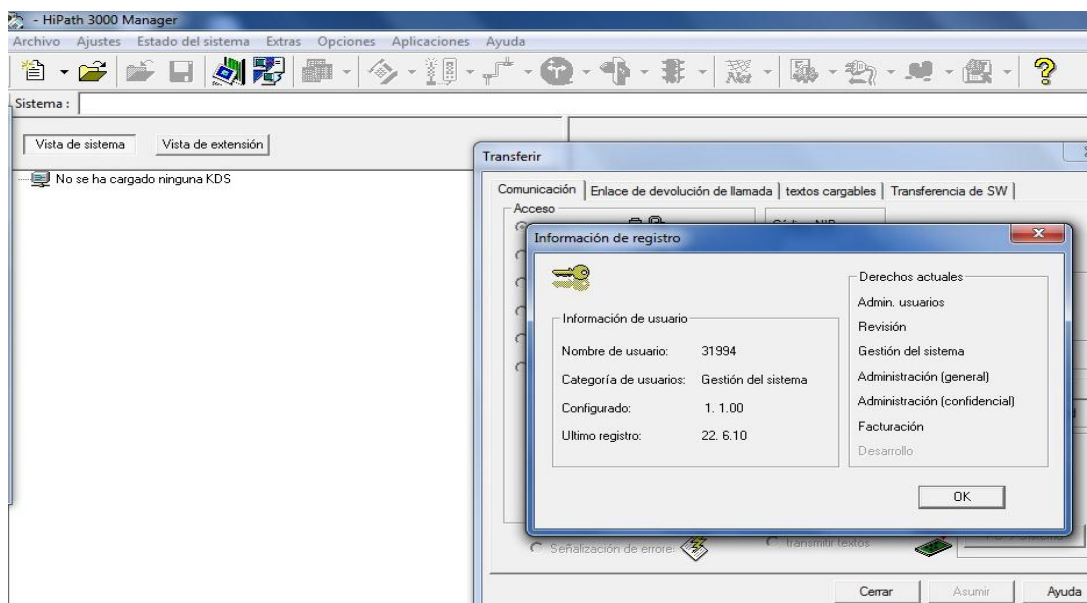


Fig. 5 Información de registro



11. Finalizada la descarga de la KDS, los demás íconos de la barra de herramientas del sistema aparecerán activos, lo que representa que ya existe una KDS cargada al programa lista para ser administrada.
12. Observe que la pantalla está dividida en dos ventanas. En la ventana de la izquierda aparecen dos pestañas: Vista de sistema y vista de extensión.

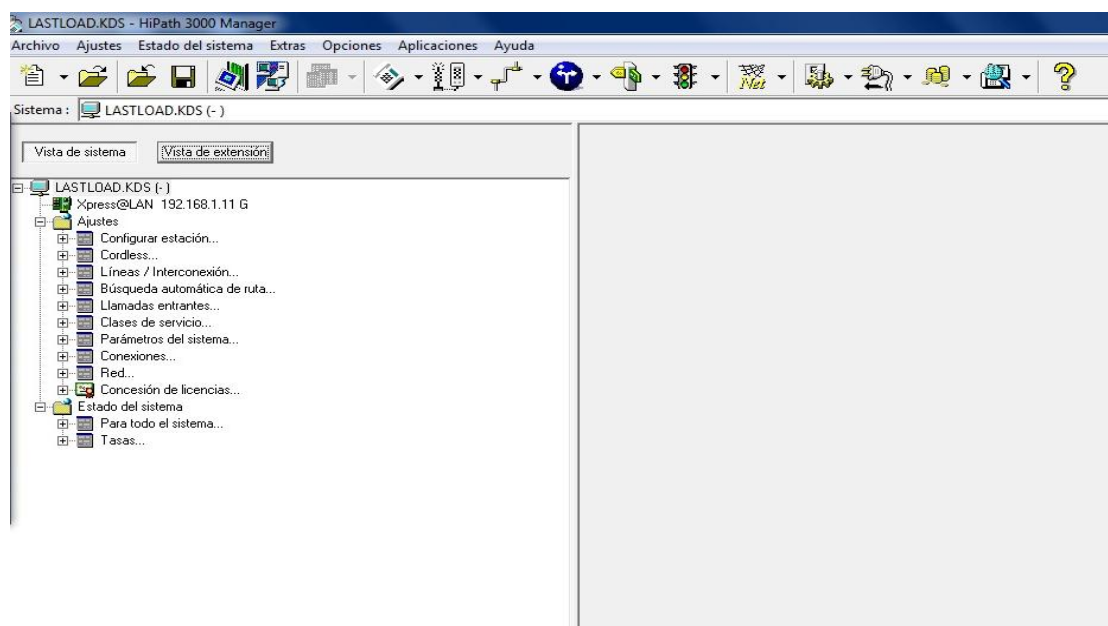


Fig. 6 Ventanas de Hipath 3000 Manager E

Actividad 4: Configuración del teléfono vía online

1. Las configuraciones del teléfono se pueden hacer a través del software. De

click en el icono transferir  se desplegará una ventana.

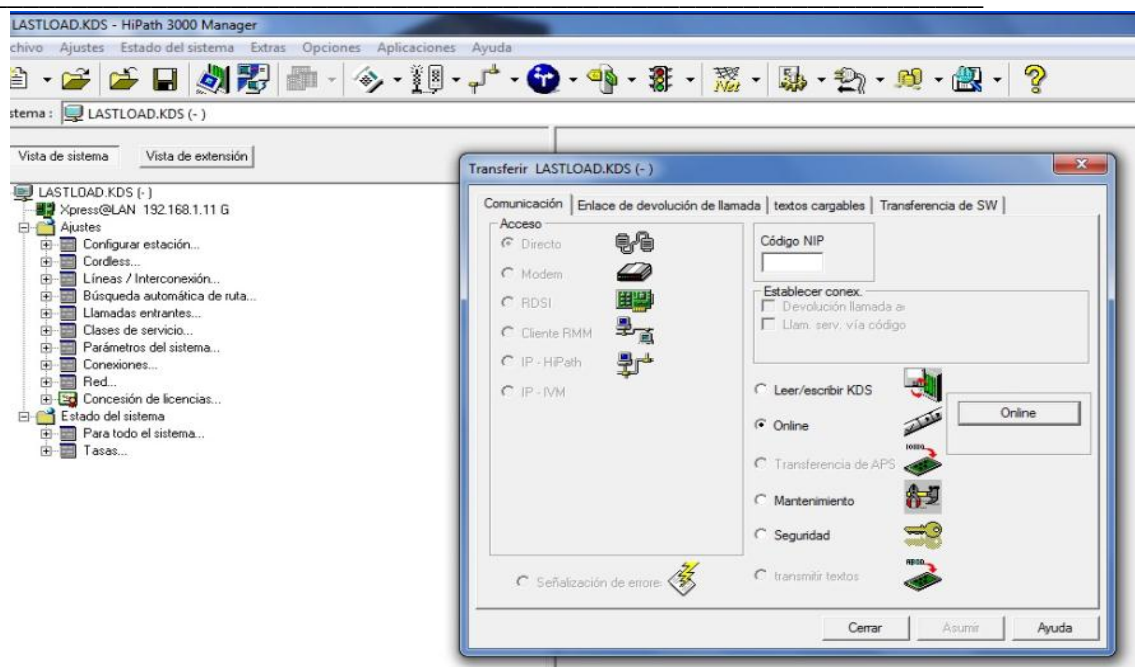


Fig. 7 Transferir/Online

2. Busque la opción online, selecciónela
3. De click en la barra que dice online. Aparecerá una ventana preguntando si se desea guardar un archivo .log a lo cual de cancelar si no se considera relevante.
4. Espere un momento hasta que aparezca un teléfono.

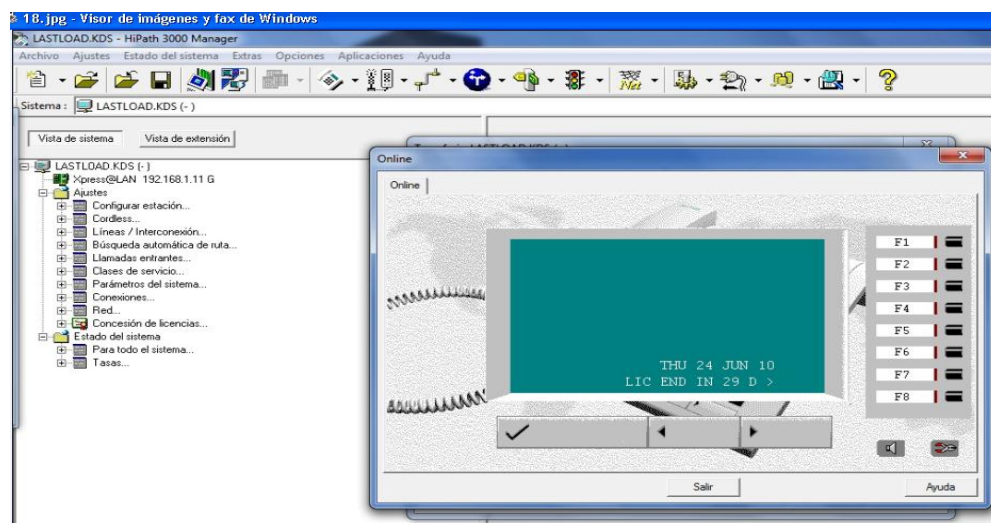


Fig. 8 Teléfono Online

5. Desde este teléfono virtual se puede configurar los teléfonos tal y como se hizo en el laboratorio 1 de DTMF.
6. Los códigos de tecla se manejan de igual modo que en DTMF.
7. Oprima *48 para seleccionar el idioma y *95 para entrar al modo de programación con el nombre de usuario y contraseña 31994. Desde aquí se administrará el sistema del teléfono.

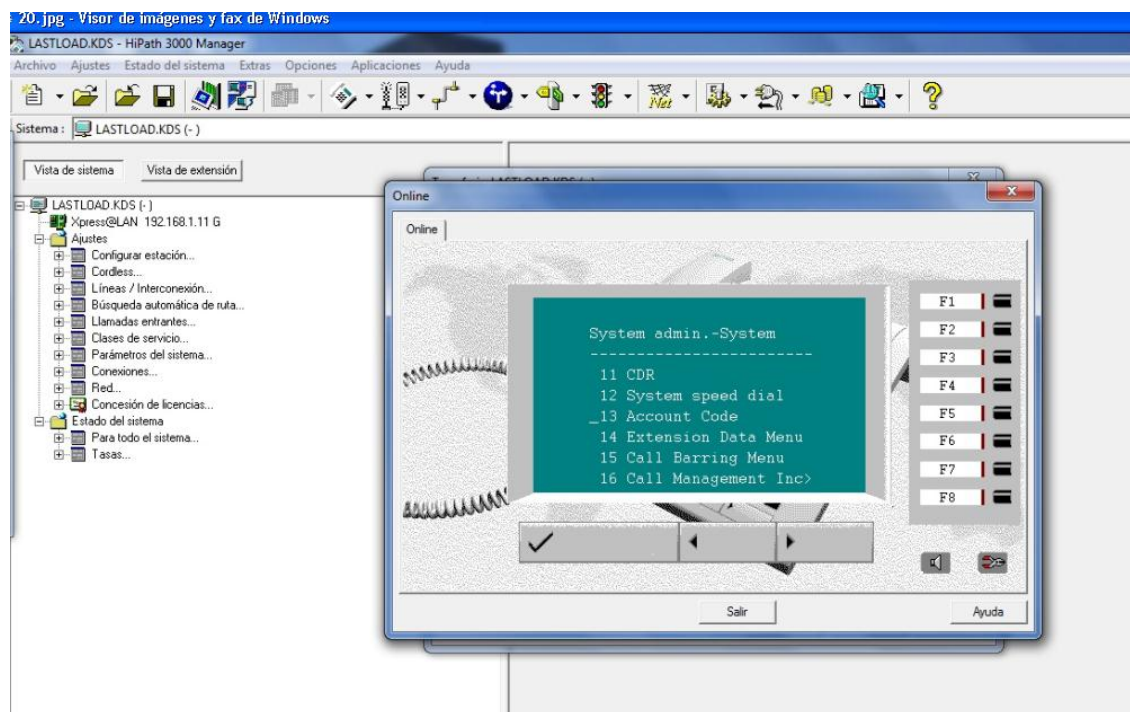


Fig. 9 Administración del sistema vía online

Actividad 5: Asignación

1. Cambie el idioma del teléfono al español y el país vía online tal y como se hizo en el laboratorio de DTMF.
2. Cambie la hora y la fecha del teléfono vía online siguiendo el mismo procedimiento instruido en el laboratorio de DTMF.

Actividad 6: Configuración de extensiones

1. En vista del sistema de click en el icono de Configurar extensión, se desplegara una ventana al lado derecho que contiene todas las extensiones. Desde esta ventana se pueden cambiar los datos de las extensiones, como el

nombre y la numeración ya que las extensiones comienzan por defecto en 100. Se pueden observar los puertos en donde están conectadas las extensiones, saber si el teléfono se encuentra activo o no y el tipo de teléfono que está conectado.

2. En estado aparecen unas pelotitas de color, cuando están en verde quiere decir que los teléfonos están conectados, en el caso de los digitales, mientras que los analógicos pueden estar o no en color verde aún estando conectados.
3. En Access se miran si los teléfonos son analógicos o digitales con las siglas SLU (Digital) o SLA (Analógico).

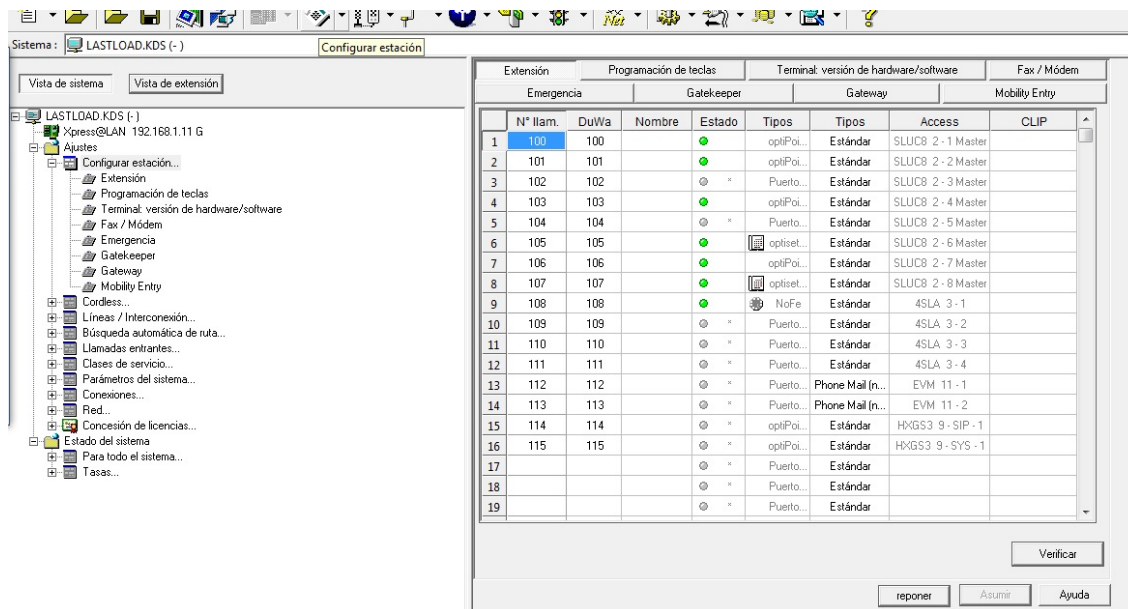


Fig. 10 Configuración de extensiones

4. Desde esta ventana se pueden cambiar los datos de las extensiones, como el nombre, la numeración ya que las extensiones comienzan por defecto en 100. Se puede observar los puertos en donde están conectadas cada extensión, también si el teléfono está activo o no y el tipo de teléfono que está conectado.
5. Modifique la numeración de las extensiones que se encuentran disponibles comenzando desde 200 dando doble click en el número de extensión anterior.
6. Elimine los números de extensiones restantes para evitar cualquier colisión.

7. En caso que se cambie el número de la extensión por uno que ya existe, se escuchará un bip indicando la repetición de dicha extensión, si este bip no se escucha se puede verificar que la extensión no se repita dando click derecho en comprobar, o bien haciendo click en verificar. A continuación se desplegará un cuadro con la información de dicha extensión y desde aquí se puede verificar si la extensión esta repetida o no.
8. Haga click en asumir para guardar los últimos cambios antes de transferir la KDS nuevamente al sistema en modo delta.

Actividad 7: Guardar cambios en el software

1. Para guardar los cambios que se hicieron en la KDS, hago click en el icono



transferir, en la pestaña de comunicación.

2. Seleccione modo delta.
3. Elija PC a Sistema para subir la KDS, preguntara si se desea guardar un archivo .log a lo cual de cancelar si no se considera relevante.
4. Espere a que se transfiera la información.

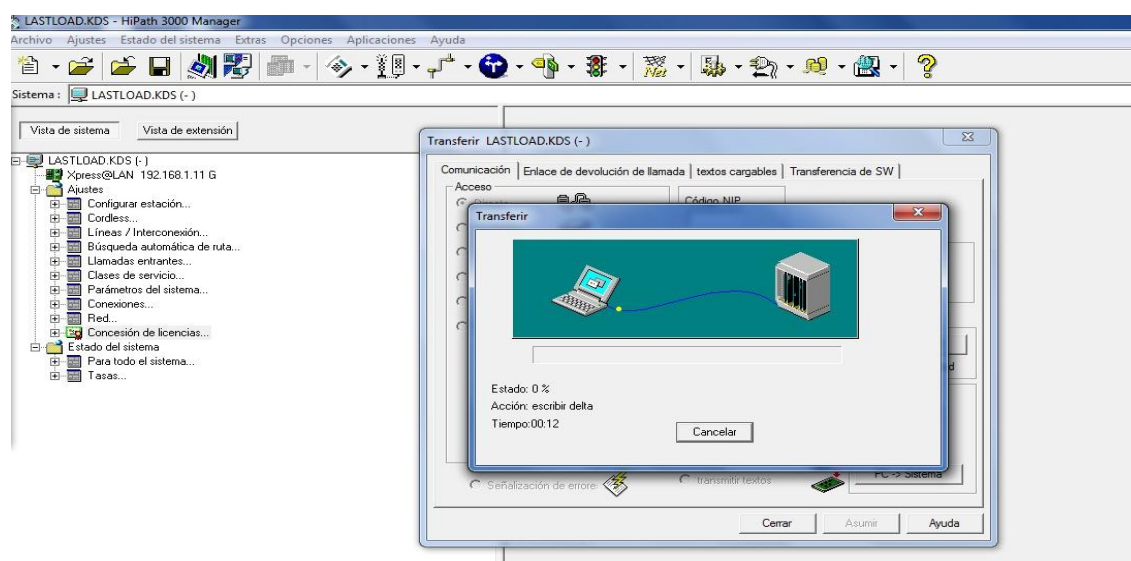



Fig. 11 Escribir delta



5. De esta manera se realizan las configuraciones básicas en el Manager E, cada vez que se realicen cambios en la central se debe repetir la actividad 5.

Actividad 8: Programación de teclas

1. Haga click en la opción Configurar estación  de la barra de herramientas.
2. Seleccione la pestaña de Programación teclas. A continuación se desplegará una ventana al lado derecho de la pantalla que contiene un teléfono que es análogo al teléfono real conectado en la extensión.
3. En la opción de programación teclas se desplegará un cuadro con todas las extensiones disponibles.
4. Las extensiones que tienen conectado un teléfono aparecen marcadas con un asterisco.
5. Al seleccionar la extensión aparecerá el teléfono que se encuentra conectado en ella, en el teléfono aparecerán las teclas que se pueden modificar.
6. Al lado del teléfono debajo de vista de extensiones aparece la ocupación actual de la tecla, y debajo de la ocupación aparece código de tecla,
7. En código de tecla se encuentran los servicios que se pueden programar en la tecla. En una misma extensión se pueden programar varias teclas.
8. Ubíquese en la extensión 101 aparece la imagen del teléfono conectado en esta extensión.
9. De click a la tecla que se desea programar.
10. En código de tecla elija desvío de llamadas, debajo de código de teclas se muestra las diferentes opciones que tiene el servicio de desvío de llamadas.
11. Seleccione 3-Sólo llamadas internas, en sólo llamadas internas se desplegará una pestaña donde se muestran las extensiones. Esto se debe a que se tiene

que elegir la extensión a la cual se quieren desviar las llamadas entrantes de la extensión que se seleccionó previamente.

12. Elija la extensión 100.
13. Elija check y luego asumir.
14. De esta manera el desvío de llamadas queda activo en la extensión 101 y todas las llamadas a esta extensión serán desviadas a la extensión 100.
15. Programe en la extensión 102 la opción de buzón.
16. Elija check y luego asumir.
17. Repita la actividad 5.

Actividad 9.1: Verificación de las teclas programadas

1. Para que el desvío de llamadas pueda funcionar se debe tener activa la tecla en donde se programo el desvío.
2. Diríjase a la extensión 101 y oprima la tecla donde se programó el desvío de llamadas, en el display aparecerá int. to: extensión 1 tal como se muestra en la Figura 9.



Fig. 12 Desvío de llamadas



-
3. Diríjase a la extensión 102 y que su compañero se quede en la extensión 101.
 4. La persona que se encuentra en la extensión 102 marque la extensión 101, su compañero podrá observar que todas las llamadas que entran a la extensión 101 son desviadas a la extensión 1. Es decir a la 100.
 5. Inmediatamente que se llama a la extensión 101 Ambos podrán escuchar que la extensión 100 empezará a sonar.
 6. Ambos vayan hacia la extensión 100 y en el display podrán visualizar
PARA: Extensión 2
Llamada: Extensión 3
 7. Una vez comprobada que la tecla de desvío de llamadas funciona correctamente, proceda a verificar si la tecla de buzón funciona.
 8. Al igual que en el desvío de llamadas la tecla en donde se programo el buzón debe estar activa.
 9. Active la tecla en donde programo el buzón en la extensión 102.
 10. Vaya a otra extensión y que alguien se quede en la 102.
 11. Marque la extensión 102, la persona que se quedo en la extensión 102 puede notar que la llamada va directo al buzón.

Actividad 10: Asignación de servicios

1. En el lado izquierda de la pantalla del programa de click en vista de extensiones.

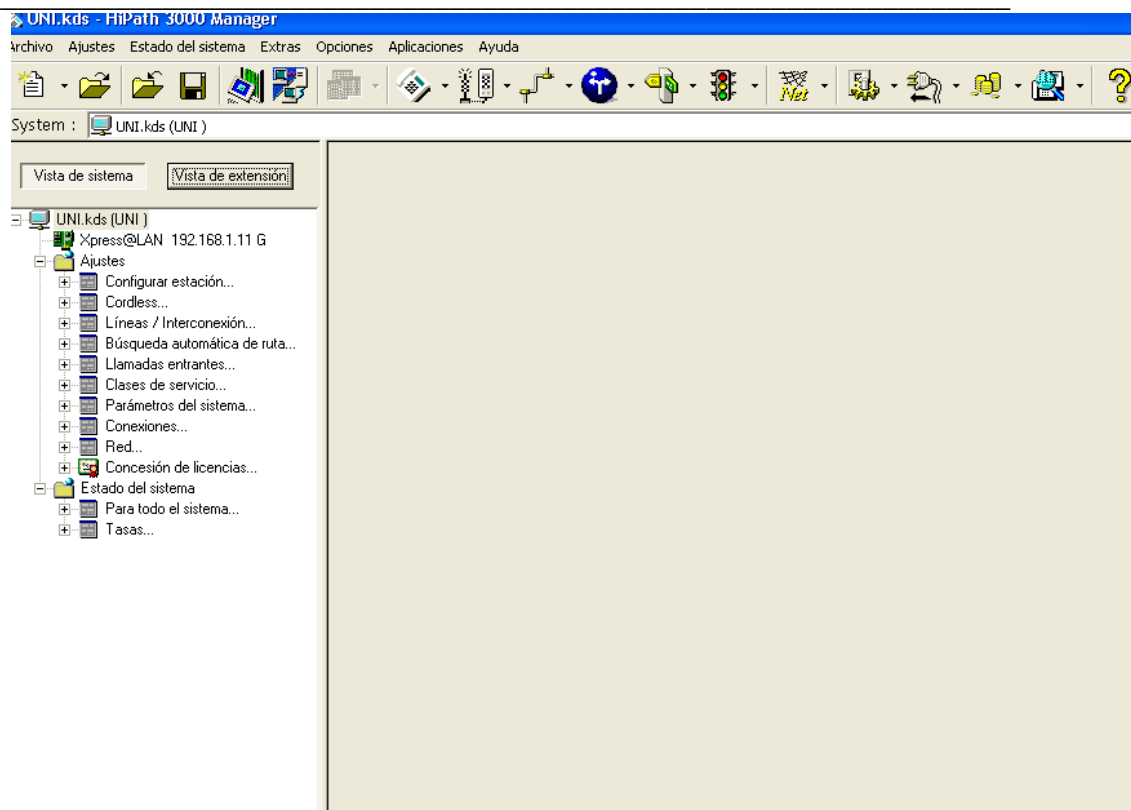


Fig. 13 Vista de extensión

2. Se desplegarán dos nuevos menús, uno en el lado izquierdo de la pantalla y otro en el lado derecho. En el menú de la izquierda se pueden ver todas las extensiones, en el de la derecha aparecen todos los servicios con los cuales pueden contar las extensiones.

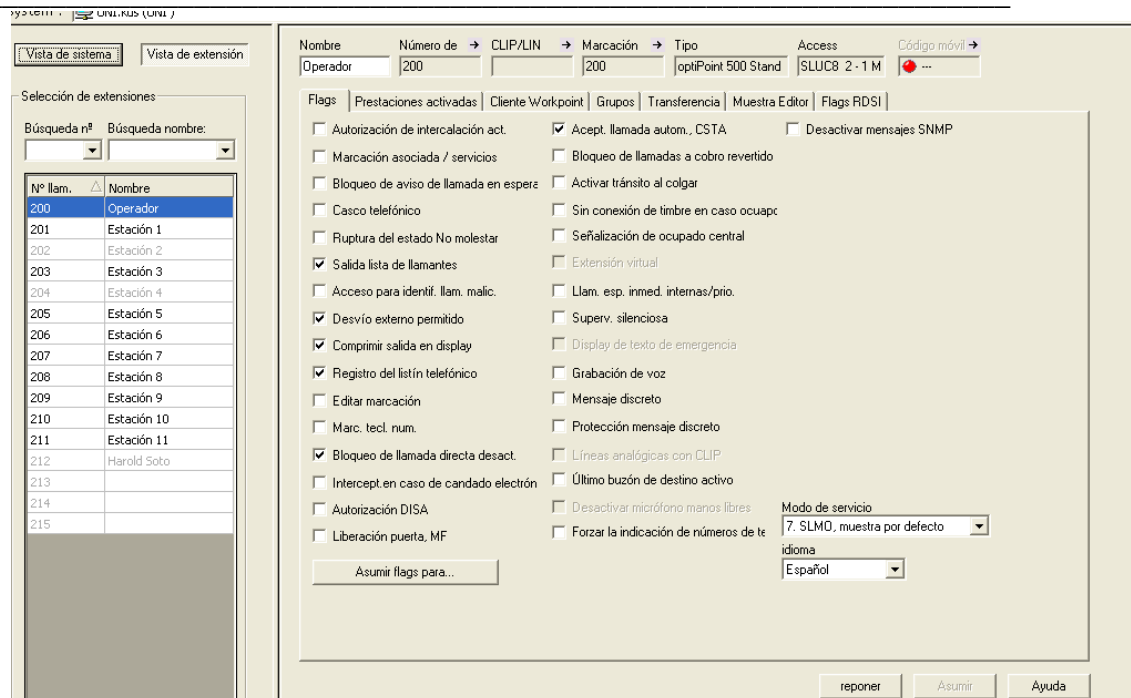


Fig. 14 Flags

3. Seleccione una extensión en el menú de la izquierda y en el menú de la derecha aparecerá toda la información relacionada con la extensión seleccionada. Este menú cuenta con varias pestañas con diferentes tipos de servicio que se pueden activar en la extensión seleccionada.
4. Desde este menú se pueden activar diferentes servicios, en esta ocasión se activara el Hotline.
5. De click en la pestaña Prestaciones activas, busque hotline. En Hotline se observan dos opciones, una llamada modo y otra Hotline.
6. En modo se pueden elegir dos opciones Hotline y socorro. Elija Hotline
7. En Hotline se elige el número de hotline que se quiere tener activos.
Seleccione 1
8. De click en asumir.

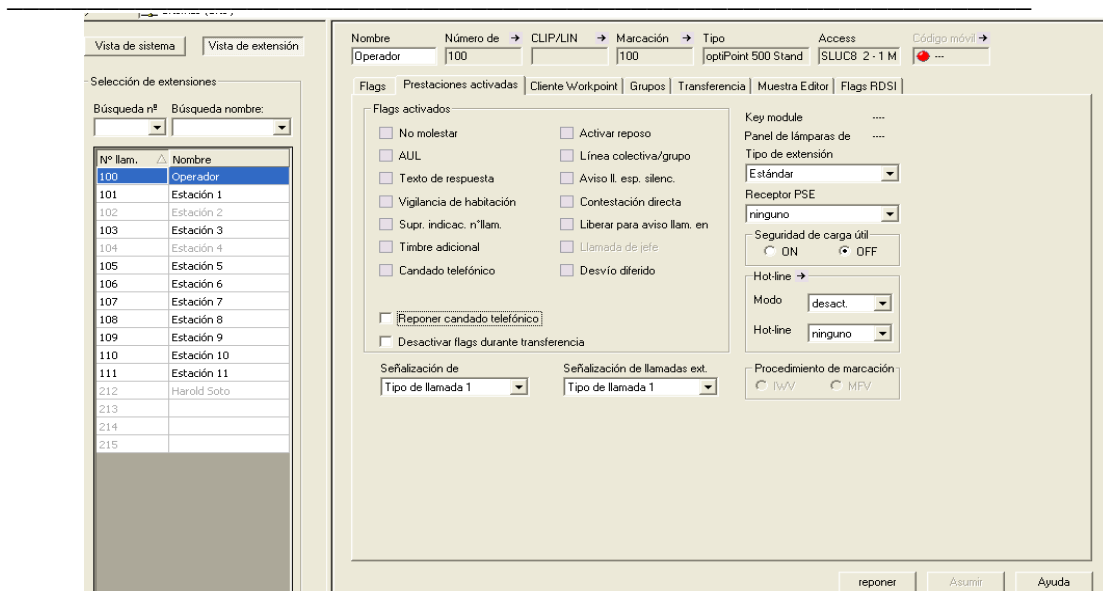



Fig. 15 Hotline

9. De click en el icono parámetros del sistema  , se desplegará una ventana en la parte derecha de la pantalla, donde aparecerán varias pestañas.
10. Seleccione ajustes del sistema, busque hotline.
11. En hotline se tiene una ventana con el mismo nombre la cual contiene una lista de los Hotline que se pueden utilizar. El hotline que se elija dentro de la lista debe ser el hotline que se eligió en la lista anterior de Hotline en prestaciones activas.
12. Elija el número de destino del Hotline y el tiempo. Este tiempo es la cantidad de segundos que se tendrá desde que se levanta el auricular para marcar cualquier número antes que se marque el hotline.
13. De click en asumir.
14. Enviar la KDS nuevamente al sistema en modo delta.

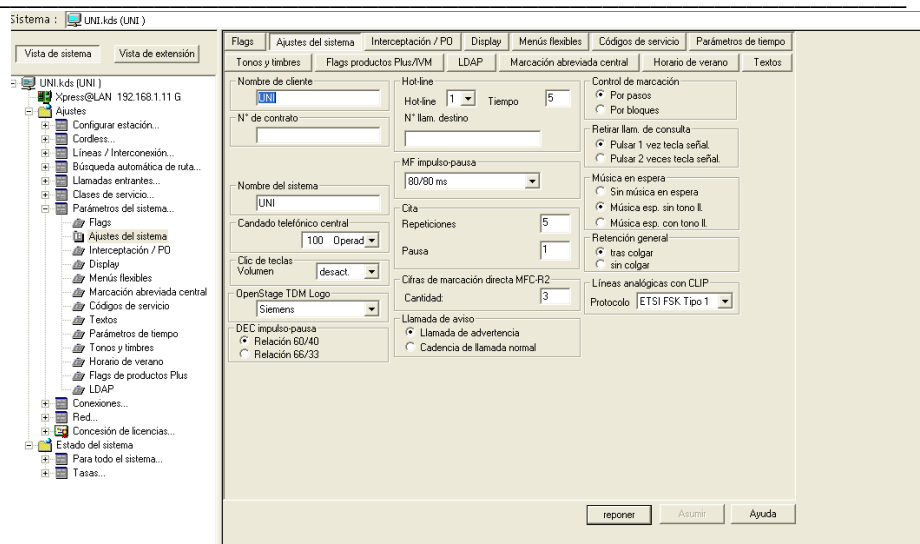


Fig. 16 Ajustes del sistema

VII. Preguntas de control

1. ¿Cuáles es el tipo de modem, el tipo de cable, el puerto y la velocidad de transmisión que se utilizan como parámetros del sistema para la conexión del servicio de PC?
2. ¿Cuándo se utiliza el modo Delta?
3. ¿Qué funciones aparecen en el menú de administración del sistema del teléfono vía online que no aparecen en el teléfono al programar vía DTMF?

VIII. Orientaciones del reporte de laboratorio

Adjunte un esquema que contenga cada una de las pestañas de las opciones de la barra de herramientas del HiPath 3000 Manager E V8.

Adjunte el diagrama del hardware de la PBX Hipath 3000.

Adjunte el diagrama del Teléfono Siemens Optipoint 500 Standard.

Se deberá seguir el formato de informes de laboratorios. Además se deben presentar las respuestas de las preguntas de control.

IX. Bibliografía

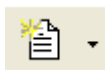
Siemens Communications, HiPath 3000 Manager E © Siemens AG 2006.



X. Anexos

XI. Explorando Hipath Manager V8.0

MENÚ DE ARCHIVO



Generar KDS nueva

Permite crear una KDS desde el inicio.



Abrir

Permite abrir un archivo de base de datos KDS del disco duro o de cualquier dispositivo de almacenamiento. (Pueden abrirse varias KDS simultáneas)



Cerrar KDS

Permite cerrar el archivo de base de datos KDS activo.



Guardar KDS

Permite salvar el archivo de base de datos KDS activo.



Transferir

Se utiliza para cargar la configuración del sistema de comunicaciones a la central y viceversa. A continuación se describe la pestaña correspondiente a comunicación que es el eje de la transferencia de archivos.

- Pestaña comunicación

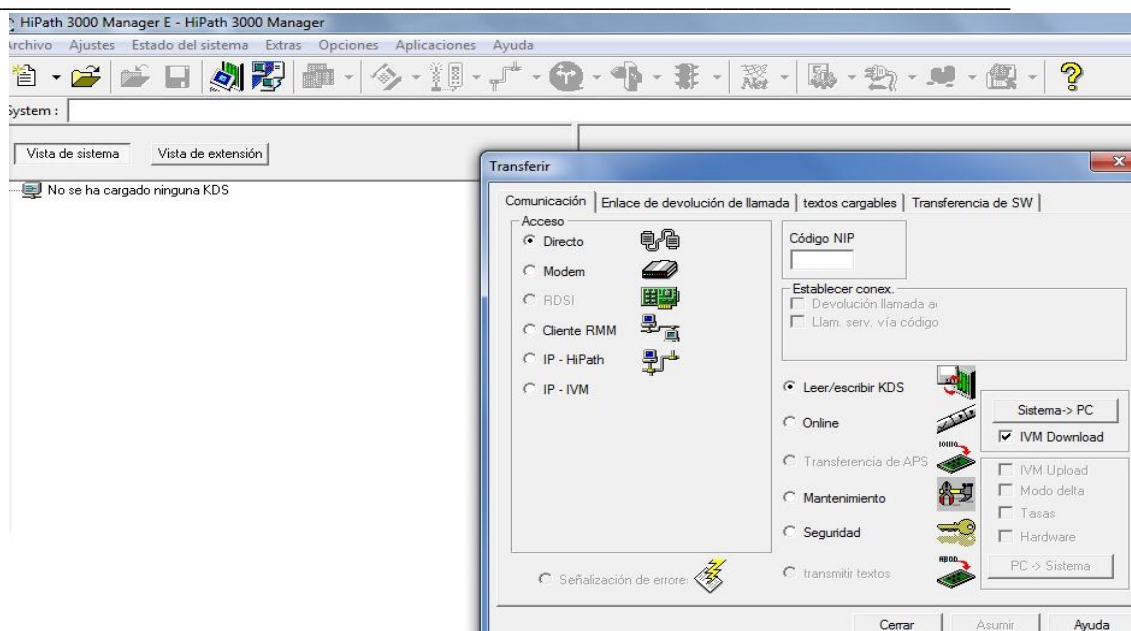


Fig. 17 Transferir

DIRECTO: Esta opción se utiliza cuando la PC se encuentra directamente conectada al sistema de comunicación, dicha PC debe estar conectada este sistema través de un cable DB9.

MODEM: Se usa cuando se tiene una conexión modem entre el sistema de comunicaciones y la PC. Al elegir esta opción el sistema de comunicación despliega un cuadro de texto dentro del cual se debe ingresar un número telefónico.

RDSI: Esta opción solamente se encuentra disponible si la PC esta equipada con una tarjeta y si se encuentra instalado el archivo capi.dll. Con esta opción el sistema de comunicación se accede vía canal B.

CLIENTE RRM: Esta opción hace posible el acceso al sistema de comunicación vía una maquina de administración remota. Dicha conexión entre la PC y el servidor RRM ocurre vía LAN.



IP-HIPATH: Esta opción hace posible el acceso al sistema de comunicaciones vía LAN a través de la tarjeta HG 1500 o la interface LAN.

IP-IVM: Esta opción habilita el acceso LAN a la IVM (correo de voz integrado) a través conexión directa LAN.

MODULO DELTA: Sirve solo para los cambios que fueron hechos desde la última vez que la base de datos fue cargada. El tiempo de transmisión es reducido drásticamente.

MODULO ONLINE: Permite hacer cambios a la base de datos del sistema de comunicaciones en tiempo real.

MANTENIMIENTO: Se usa para cambiar las configuraciones que son necesarias para el mantenimiento remoto del sistema de comunicaciones.



Transferir servidor Hipath 5000 RSM/AllServe

Se utiliza para cargar la configuración de los servidores en HiPath 3000 Manager y transferir la configuración modificada de nuevo al servidor.



Datos de toda la red

Se utiliza para definir parámetros específicos para todas las estaciones de un sistema en red. Los datos que pueden ser modificados aquí deben ser coherentes en la red para los sistemas de comunicación individual.

MENÚ DE CONFIGURACIÓN



Configurar estación

Se utiliza para ver y definir o editar las configuraciones de las extensiones.



Configurar cordless

Se usa para establecer los parámetros de los cordless



Líneas / Interconexión

Se determinan los parámetros relacionados con las troncales, rutas y RSDI



Búsqueda automática de ruta

Habilita al sistema de comunicación para controlar automáticamente por cual ruta saldrá la llamada saliente. La llamada puede ser enrutada por un canal público o privado. Esto asegura que la conexión más costo-efectiva sea usada.



Llamadas entrantes

Se usa si la extensión no responde a una llamada dentro de un tiempo dado.



Clases de servicio

Se usa para restringir llamadas externas.



Configuraciones de red

Se utiliza para definir los ajustes necesarios para conectar el sistema de comunicación a una LAN.

- **Acceso IP**

Protocolo

Se pueden seleccionar los siguientes protocolos:

LIM: En este modo la sub-tarjeta LIM en la tarjeta de control es utilizada como un acceso LAN para el sistema de comunicación.

HIP: En este modo se utiliza la tarjeta HG 1500. Esta tarjeta trabaja en modo puente que es el HG 1500 y la tarjeta central del sistema de comunicaciones las cuales tienen diferentes direcciones ip pero que comparten una interfaz física LAN.

SLIP: El acceso se habilita a través de la interfaz V.24. El router así como el CommServer (V.24/IP box) no se pueden conectar aquí. Esta opción es utilizada sólo en conexión con la Hipath 500 por medio de una tarjeta HXGO con interfaz V.24.



Parámetros del sistema

Se configuran todos los parámetros del sistema.



Conexiones

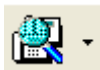
Permite configurar los puertos del sistema (troncales) para soportar una amplia gama de equipos auxiliares (módulos).



Tasas

Incluye la recopilación y generación de registros de datos de las llamadas entrantes

y salientes. Las funciones CDR (Call Detail Records) y SMDR (Station Message Detail Records) proporcionan información sobre las llamadas externas desde y hacia el sistema de comunicación. El formato de registro de llamadas se determina mediante el uso de banderas de todo el sistema de ajuste en el formato de salida.



Para todo el sistema

Esta opción contiene una serie de pestañas, que afectan el estado del sistema de comunicación de varias maneras. Algunas de estas pestañas son sólo para propósito informativo, mientras que otras le permiten hacer cambios a los parámetros que aparecen. El estado del sistema de comunicación involucrado aquí es el estado en el momento cuando se descarga la base de datos del cliente.

MENÚ DE AYUDA



Ayuda

Abre un cuadro de diálogo que muestra los siguientes detalles sobre el programa:

- Nombre del programa.
- Número de versión.



- Empresa.
- Derecho de Autor.
- Los sistemas de comunicación compatibles.



Laboratorio No. 3: Introducción a Hipath 2000 *

Modulo	Telefonía IP		
Tipo Práctica	<input type="checkbox"/> Laboratorio <input type="checkbox"/> Simulación		
Unidad Temática			
No Alumnos por práctica	2	Fecha	
Nombre del Profesor			
Nombre(s) de Alumno(s)			
Tiempo estimado		Vo. Bo. Del Profesor	
Comentarios			

Objetivos de la práctica de laboratorio

I. Objetivo general

1. Examinar la operación de la central telefónica PBX Hipath 2000 mediante Web-Based Management.

II. Objetivos específicos

1. Realizar configuraciones básicas de la central PBX Hipath 2000.
2. Validar extensiones SIP en teléfonos softphones.
3. Efectuar la llamada entre los teléfonos softphones.

III. Medios a utilizar

- PBX Hipath 2000
- Equipo de cómputo
- Switch
- Softphone Zoiper o Xlite
- Java ultima version

IV. Introducción

Este laboratorio es una introducción al funcionamiento de la central telefónica Hipath 2036. HiPath 2000 es un sistema puro de comunicaciones IP desarrollado en LINUX, una arquitectura de software abierto. La comunicación IP con HiPath 2000 ofrece seguridad, alta calidad, flexibilidad y gran disponibilidad.



La administración de la central Hipath 2000 se realiza vía Web conocido como Web-Based Management (WBM).

La telefonía IP utiliza diversas funciones de seguridad habituales en el ámbito de las comunicaciones de datos que también protegen las comunicaciones de voz frente a piratas informáticos y virus.

HiPath 2000 ofrece una máxima seguridad ya que la calidad de Servicio (QoS) garantiza una alta calidad de voz de forma constante y otorga siempre la máxima prioridad a la comunicación de voz frente a las comunicaciones de datos. De esta manera, las empresas no tienen que renunciar a ninguna de las características actuales de la telefonía digital TDM sino que, además, pueden aprovechar todas las ventajas de las comunicaciones IP.

V. Conocimientos previos

- Telefonía IP
- Centrales IP
- Protocolo SIP
- Adaptadores ip y diversos tipos que existen
- Softphones
- Diagrama del hardware de la central Hipath 2000.

VI. Procedimiento

El escenario a implantarse se muestra en la figura 1. Aquí se presentan los medios a utilizar como son la centralita Hipath 2000 modelo 2036 y los softphones:

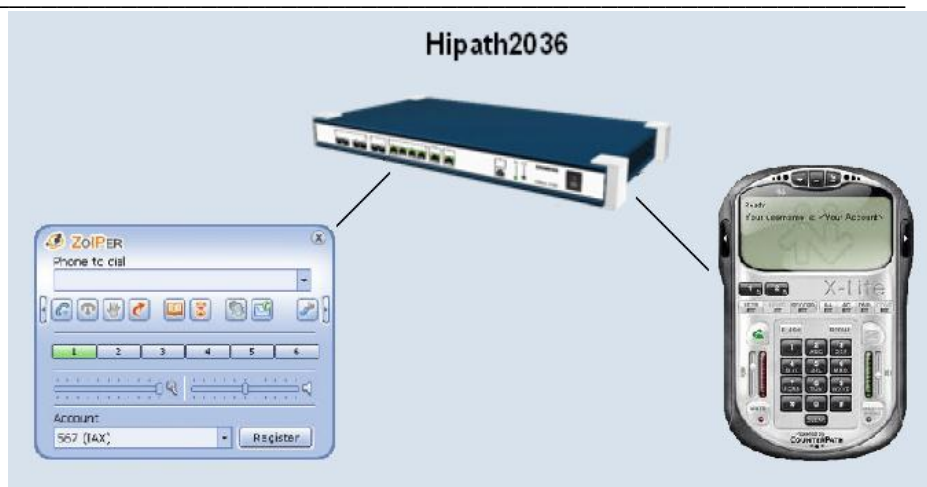
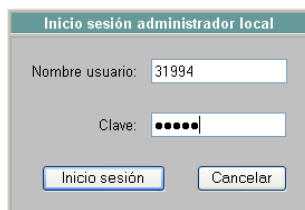


Fig. 1 Escenario del laboratorio

Actividad 1: Configuraciones básicas

1. Conecte la centralita Hipath 2000 al suministro eléctrico y oprima el switch de encendido/apagado.
2. Conecte el puerto LAN de la computadora al switch.
3. Abra una ventana de su explorador
4. Escriba la dirección <https://192.168.1.2>
5. Cuando la página cargue aparecerá una ventana como la que se muestra en la figura 2. Escriba el nombre de usuario y la clave. El nombre de usuario así como la clave por defecto es 31994.

HiPath 2000 V2.0



To use the English version of WBM, please change the language settings of the Internet Explorer (Internet options).

WBM precisa además los siguientes componentes:

- Java 2 (TM) con Java-Plugin2 (SUN), V1.4.2_04 JRE, descarga de [SUN Download](#)
- XML Parser 3.0 (SP5) de Microsoft, descarga de [Microsoft Download](#)
- sólo necesario cuando fracasa la instalación del XML Parser: Windows Installer V2.0, descarga de [Microsoft Download](#)

Fig. 2 Página de inicio de Hipath 2000

Actividad 2: Configuración de fecha y zona horaria

1. De click en modo experto.
2. En el menú explorador de click en Ajustes básicos.
3. Seleccione el vínculo de Fecha y hora. Aquí aparecen tres parámetros modificables como son la Fecha y hora, Ajustes zona horaria y Ajustes SNTP.
4. De click derecho en Ajustes zona horaria y seleccione Editar ajustes zona horaria.
5. A continuación busque el ajuste de zona horaria correspondiente a (GMT - 6:00) América Central, luego haga click en Asumir.
6. De click derecho en Fecha y hora y seleccione Ajustar fecha y hora.
7. El formato a seguir es Mes/Día/Año y la hora en Hora/Minutos/Segundos. En la pantalla aparece DD/MM/AAAA pero se debe seguir el formato antes mencionado para la configuración. Haga click en Asumir una vez confirmados los cambios.
8. Seleccione Guardar en el disquete ubicado en la parte inferior de la pantalla.



9. Reinicie la central presionando el botón reset de la central por un período de 5 segundos.
10. Espere que la central cargue nuevamente su configuración. Esto puede dilatar de 5 a 10 minutos.
11. Luego ingrese a la dirección de la página web de la central y en modo experto, seleccione Explorador y después Ajustes básicos.
12. En Administración de licencias observe que las prestaciones de la Hipath 2000 tienen un período de evaluación de 30 días. En este período se pueden validar las extensiones que se deseen. Como la central tenía fecha de 1999 todas estas licencias estaban expiradas por lo que era imposible validar extensiones bajo estas condiciones.

Actividad 3: Anadir extensiones en la Hipath 2000

1. En modo experto en el menú explorador de click en Extensión. Cargará una ventana al lado derecho de la pantalla en el cual se observa una carpeta llamada extensión
2. De click en la carpeta llamada extensión, se desplegaran tres carpetas mas, llamadas extensión, programación de teclas y servicio emergencia
3. De click derecho a la carpeta extensión, así como se muestra en la figura 3.
4. De click en editar tabla de extensiones.

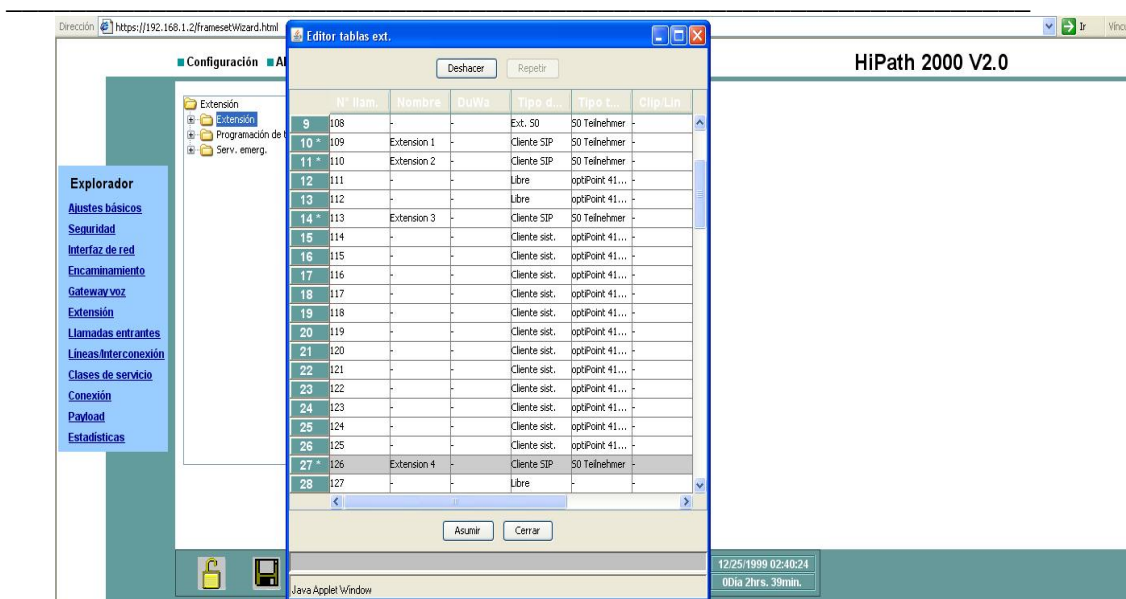


Fig. 3 Añadir extensiones

5. En la ventana de las extensiones aparecen varias casillas como el número de la extensión, el nombre y el tipo de extensión a crearse.
6. Cree extensiones desde la 109 hasta la 113.
7. Haga doble click en la casilla nombre para modificar el nombre de la extensión. Introduzca el mismo número de la extensión.
8. En tipo seleccione cliente SIP.
9. Una vez creadas todas las extensiones de click en asumir.
10. Cierre la ventana que se desplego y luego de click en el símbolo + de la carpeta que dice extensión. Se desplegara una serie de nuevas carpetas con los distintos tipos de extensiones que se pueden crear en la central.
11. De click en cliente SIP, observara las extensiones creadas anteriormente.

Siempre que se realice algún cambio o modificación de click en el icono de guardar, el cual se encuentra en la parte inferior de la pantalla y corresponde a la imagen de un disco.

Actividad 4: Comunicación entre softphones

1. Registre el softphone X-Lite y Zoiper validos en la central Hipath 2000 es decir en la dirección 192.168.1.2.



Fig. 4 X-Lite

2. Para registrar el softphone X-Lite haga click en la pestaña que se muestra en la figura 4, donde aparece Show Menu y luego en la opción SIP Accounts Settings...
3. Haga click en Add nueva cuenta y llene los parámetros tal como se muestra en la figura 5. Tomando como referencia la extensión número 110.
4. El nombre que aparece en el display, el nombre de usuario, la contraseña y la autorización del nombre de usuario se completan introduciendo el número de extensión.
5. El dominio corresponde a la dirección IP de la central Hipath 2000 en este caso.
6. En domain proxy se deja también la misma dirección IP de la central Hipath 2000.

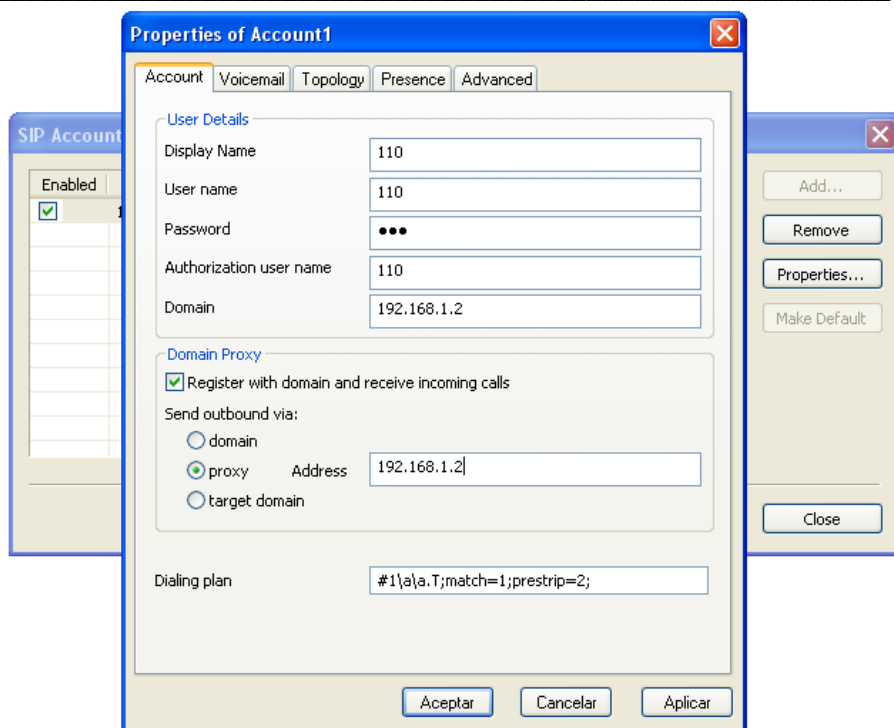


Fig. 5 Propiedades de la cuenta

7. Una vez introducidos todos los datos haga click en Aceptar y cierre la ventana de SIP Accounts en la opción close. Así le aparecerá el número de extensión debidamente registrado en el display del softphone, listo para realizar o recibir una llamada.



Fig. 6 X-Lite registrado

8. De igual manera procedemos ahora a registrar el softphone Zoiper haciendo click en el ícono de Opciones dentro del menú principal.



Fig. 7 Zoiper

9. A continuación se aparecerá una ventana como la que se muestra en la figura 8.
10. Seleccione Cuenta nueva de SIP. Le pedirá el número de la extensión. Introduzca por ejemplo la extensión número 111.

11. Ingrese los datos que aparecen en seguida: El dominio corresponde al número de la dirección IP de la central Hipath 2000, los campos de nombre de usuario, clave y el número de llamante complételo con el número de extensión 111.

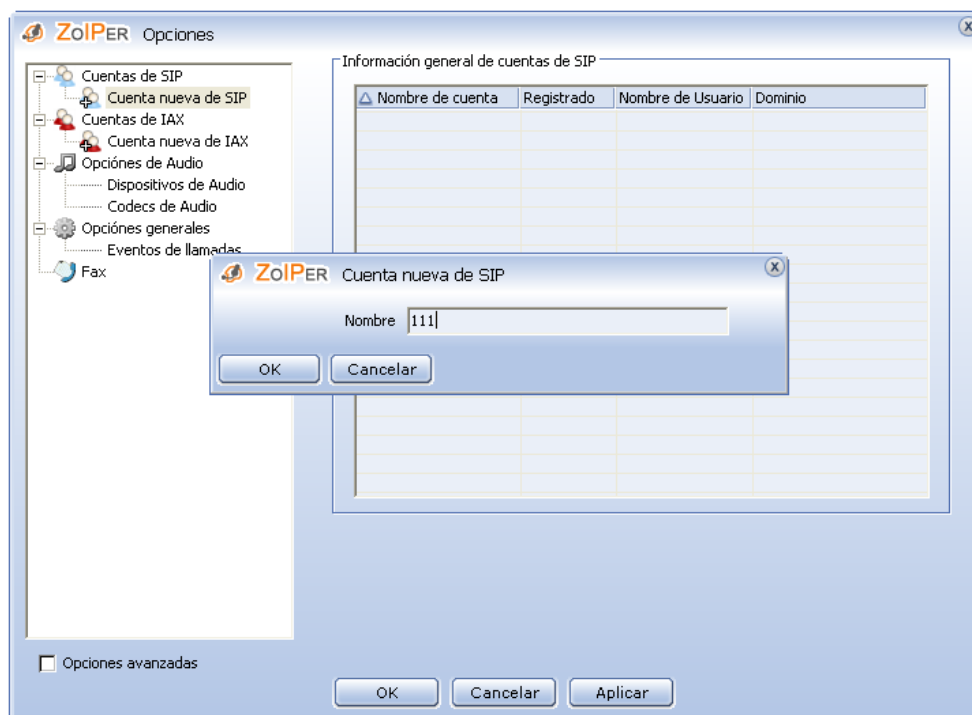


Fig. 8 Cuenta nueva de SIP

12. Una vez introducidos todos los datos haga click en OK para guardar los cambios. Así le aparecerá el número de extensión debidamente registrado en el display del softphone, listo para realizar o recibir una llamada.
13. Para hacer llamadas desde el Zoiper haga click en la viñeta de la parte derecha para desplegar un pequeño teclado para introducir los el número de extensión y luego haga click en Llamar o simplemente introduzca desde el teclado de la computadora el número de extensión y presione Enter.



Fig. 9 Zoiper registrado

14. Para hacer llamadas desde el X-Lite puede presionar los dígitos del teclado del softphone para introducir el número de extensión y luego hacer click en Dial o bien simplemente introduzca desde el teclado de la computadora el número de extensión y presione Enter.
15. Una vez que la llamada esté establecida se observará tal como se muestra en la figura 10.



Fig. 10 Establecimiento de la llamada



VII. Preguntas de control

1. ¿Qué es telefonía IP?
2. ¿Qué es softphone?
3. ¿Cuál es la diferencia entre la Hipath 2000 y la Hipath 3000?
4. ¿Cuál es la dirección web que trae por defecto la Hipath 2000?
5. ¿Cuál es el protocolo que utilizan las extensiones IP en la Hipath 2000?



Laboratorio No. 4: Configuración Hipath 2000 y adaptador ATA Linksys Cisco

Modulo	Redes de Telefonía		
Tipo Práctica	<input type="checkbox"/> Laboratorio <input type="checkbox"/> Simulación		
Unidad Temática			
No Alumnos por práctica	2	Fecha	
Nombre del Profesor			
Nombre(s) de Alumno(s)			
Tiempo estimado		Vo. Bo. Del Profesor	
Comentarios			

Objetivos de la práctica de laboratorio

I. Objetivo general

1. Configurar el adaptador ATA en la PBX virtual Asterisk.

II. Objetivos específicos

1. Instalar el servidor Asterisk a través de una máquina virtual.
2. Añadir extensiones SIP.
3. Registrar el adaptador ATA en una extensión de la PBX
4. Establecer la comunicación entre softphones y Adaptador ATA cisco

III. Medios a utilizar

- Equipo de cómputo
- Router o Switch
- Disco de instalación de Trixbox
- Adaptador ATA cisco
- Teléfono analógico
- Softphone Zoiper o Xlite



IV. Introducción

Asterisk es una completa central PBX basado en software, bajo el sistema operativo Linux Centos que permite construir aplicaciones de comunicaciones tan complejas o avanzadas como se desee sin incurrir en altos costos y con más flexibilidad que cualquier sistema de telefonía.

Linux Centos es la distribución de linux que sirve como Sistema Operacional, está basado en Linux Red Hat Enterprise.

Asterisk es el núcleo de telefonía y cuando hablamos de Asterisk incluimos también los drivers de Zapata Telephony (zaptel) y la librería para soporte RDSI.

Este laboratorio empieza desde la instalación del servidor Asterisk. Luego de la instalación se procede a asignarle una dirección IP dentro de la red de la facultad procurando no crear conflicto con una dirección que ya se encuentre ocupada.

La administración de la central Asterisk se realiza vía web, introduciendo la dirección IP asignada en la máquina virtual en el explorador. Se crean extensiones SIP que luego se validan en los softphones para establecer una llamada.

Asimismo se instalan los módulos que se pueden agregar en el Asterisk.

V. Conocimientos previos

- Máquina Virtual
- Asterisk
- Comandos de Asterisk
- Servicios que brinda Asterisk.



VI. Procedimiento

Actividad 1: Instalación del sistema operativo Linux

1. Inserte el cd de Trixbox y haga click en crear una nueva máquina virtual.
2. Inmediatamente va a detectar el Trixbox en Disco Instalador y de click en siguiente.
3. Seleccione el sistema operativo y la versión correspondiente, la cual es Linux y CentOS respectivamente. Pide el espacio máximo del disco duro.
4. Seleccione la opción de encender la máquina virtual inmediatamente después de la instalación en “Power on this virtual machine”.
5. Inmediatamente después de la instalación cargará el trixbox
6. Seleccione el teclado, en este caso Estados Unidos.
7. Elija la zona horaria
8. Presione ok.
9. Se le pedirá una contraseña, luego de confirmar su contraseña iniciará el formato de su disco duro y la instalación de los paquetes. El tiempo de esta dependerá de la capacidad del PC.
10. Una vez que se termina la instalación se le pedirá el nombre de usuario el cual es root y un password, que viene a ser el que se definió anteriormente. Tal como se muestra en la figura 2.

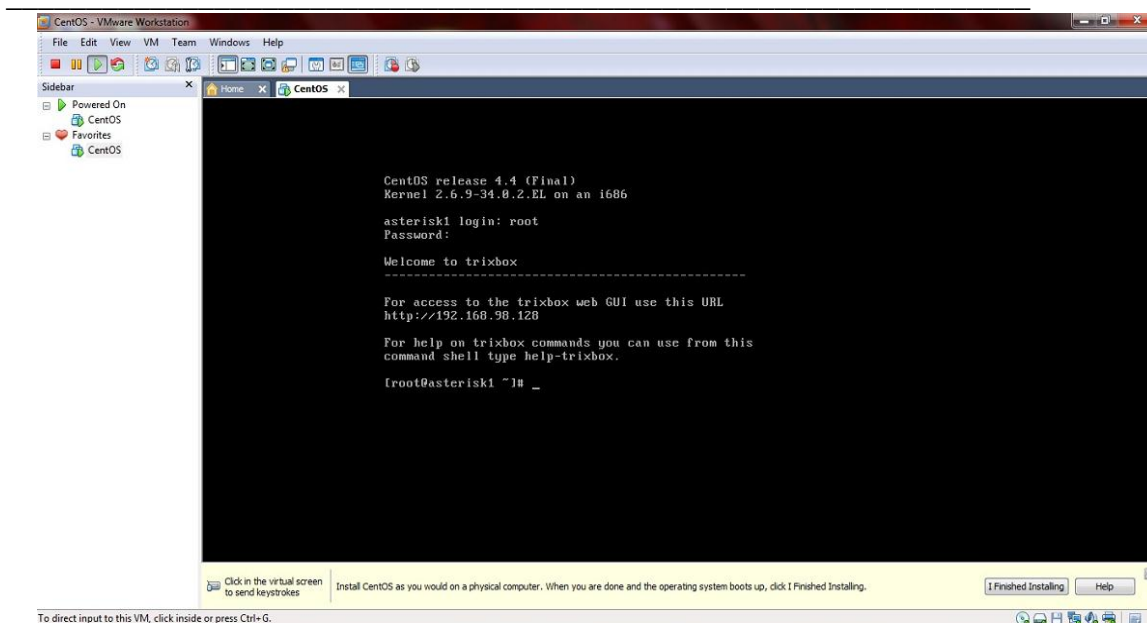


Fig. 1 Asterisk login

11. Cuando la instalación termine apague la máquina virtual con el comando “shutdown -h now”.

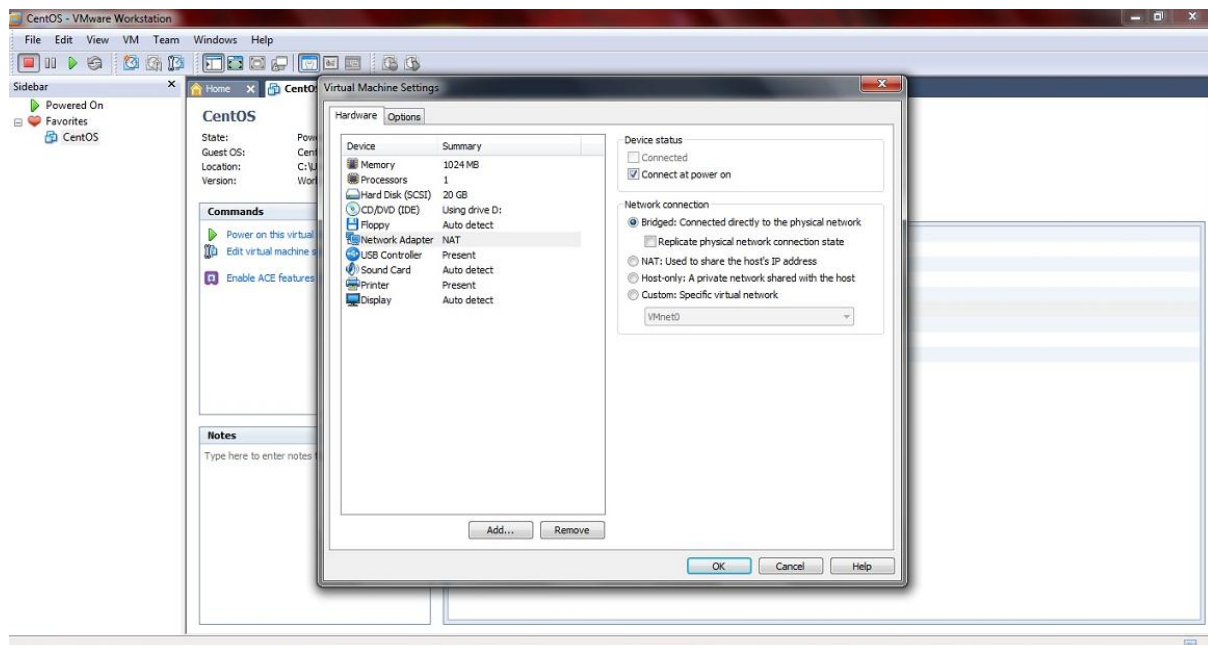


Fig. 2 Instalación de máquina virtual



12. Luego se debe cambiar en el sistema operativo CentOS pestaña de dispositivos, opción adaptador de red la conexión de red NAT por Bridged tal como se muestra en la figura 1.

Actividad 2: Configuración de la dirección IP del Asterisk

1. Cuando cargue el sistema operativo Linux Centos aparecerá el login para ingresar al asterisk y luego el password. El login es root mientras que la contraseña es definida por el usuario. En este caso la contraseña es electrónica.
2. Para salir de Asterisk presione Control + Alt
3. Inicialice la aplicación Advanced Port Scanner para detectar todas las direcciones IP que se encuentran ocupadas dentro de la red de la UNI.
4. Elija una dirección que no se encuentra ocupada dentro del rango 192.168.73.1 hasta 192.168.73.255. En este caso elegimos 192.168.73.3.

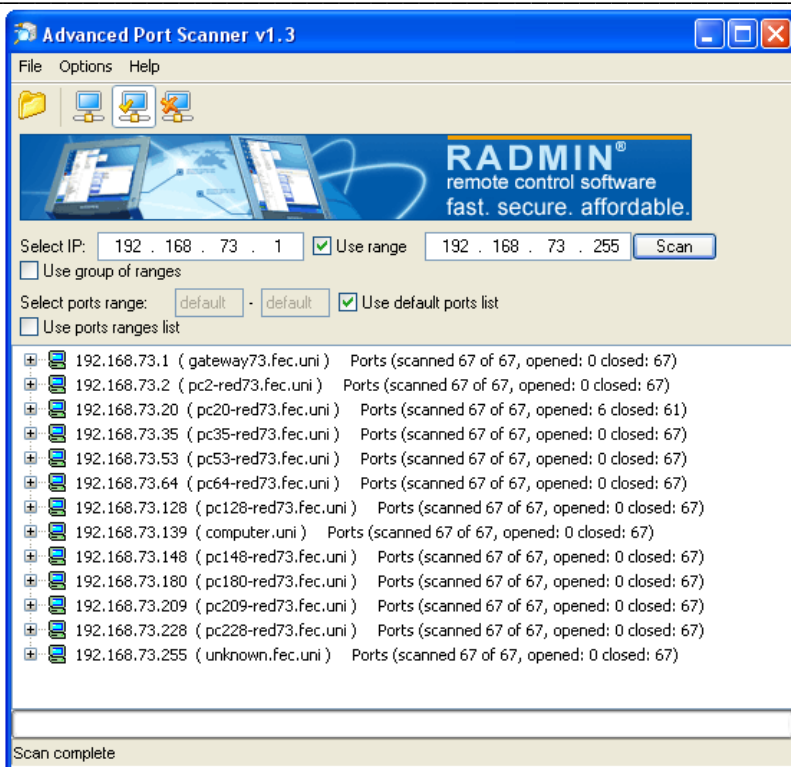


Fig. 3 Advanced Port Scanner v1.3

- Introduzca el comando netconfig para cambiar la dirección IP que contiene por defecto el Asterisk y presione yes.



Fig. 4 Comando netconfig

6. Ingrese los parámetros de configuración IP.
7. Establezca la dirección IP en 192.168.73.3; máscara 255.255.255.0 y tanto el Gateway por defecto como el primary name server en 192.168.1.1.
8. Presione ok.

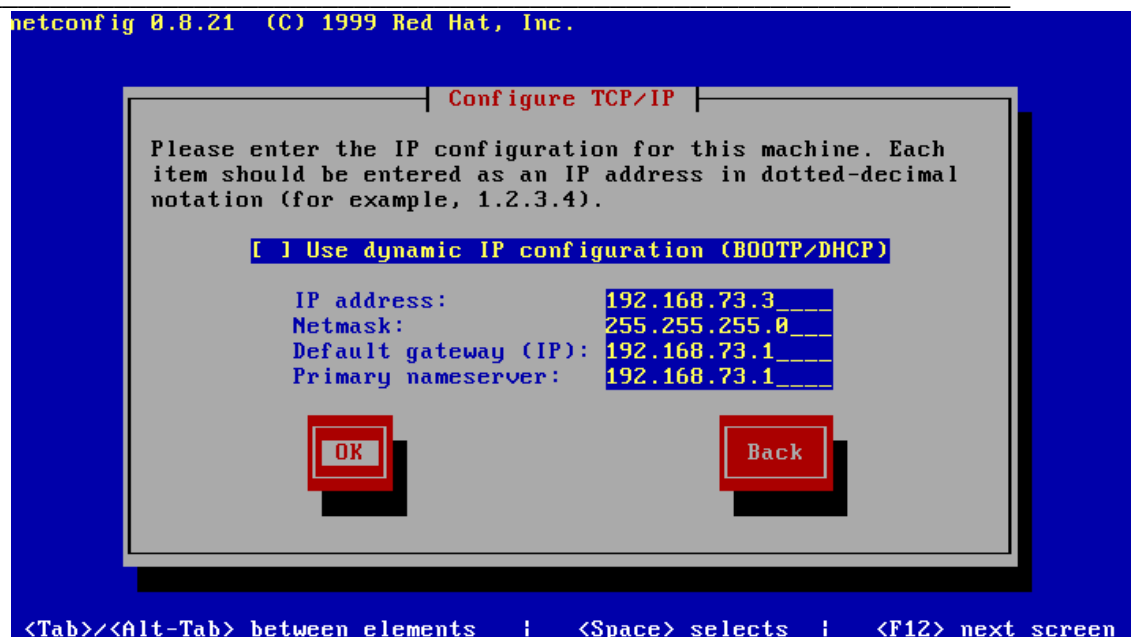


Fig. 5 Configuración TCP/IP

9. Luego escriba el comando `service network restart` para reiniciar el servicio de red.
10. Ingrese el comando `ifconfig` para verificar si la información de los parámetros IP está configurada correctamente.

```
[root@asterisk1 ~]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0C:29:F4:76:E6
          inet addr:192.168.73.2  Bcast:192.168.73.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fef4:76e6/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1149 errors:0 dropped:0 overruns:0 frame:0
          TX packets:122 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:76150 (74.3 KiB)  TX bytes:8106 (7.9 KiB)
          Interrupt:5 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:162 errors:0 dropped:0 overruns:0 frame:0
          TX packets:162 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:25839 (25.2 KiB)  TX bytes:25839 (25.2 KiB)

[root@asterisk1 ~]#
```

Fig. 6 Comando ifconfig



Actividad 3: Añadir extensiones en el Asterisk vía web

1. Abra una ventana de su explorador.
2. Escriba la dirección del trixbox definida en el Linux Centos <http://192.168.73.3>.
3. En la parte superior derecha busque Modo de usuario y haga click en el vínculo interruptor para poder entrar al Asterisk.



Fig. 7 Página principal de Trixbox

4. A continuación le pedirá un nombre de usuario y un password. El nombre de usuario es maint, el password es "password".

5. Seleccione Asterisco de la barra de menú y haga click en Free PBX para ingresar a las configuraciones.

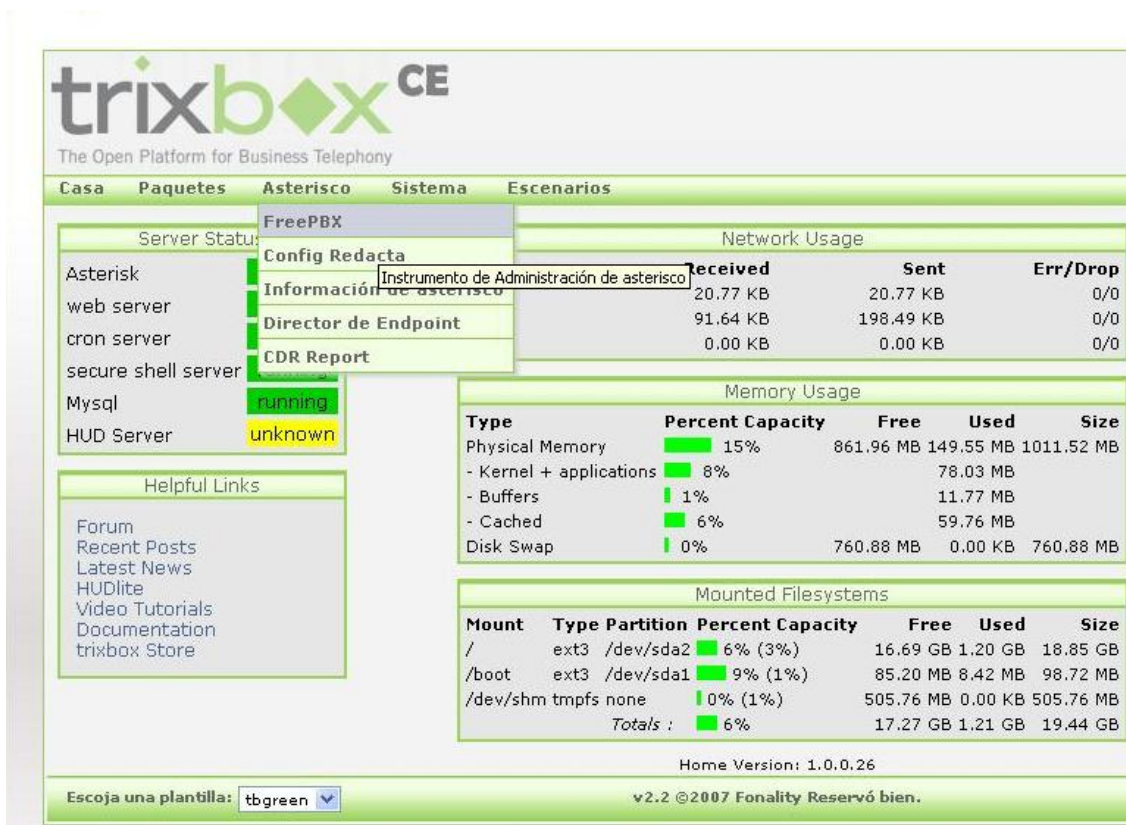


Fig. 8 Instrumento de Administración de Asterisk

6. En la parte superior derecha cambie el idioma a español.
7. Seleccione Configuración de la barra de menú y se le desplegará un pequeño menú a la izquierda.
8. En dicho menú elija configuraciones generales y configure todos los parámetros tal y como se muestra en la figura 9.
9. Cuando haya terminado con todas las configuraciones que se muestran en la figura 9 de click en enviar cambios.
10. De click en Apply Configuration Changes.



The screenshot shows the freePBX 2.2.1 web interface. The top navigation bar includes links for 'Configuración', 'Herramientas', 'Informes', 'Panel', and 'Grabaciones'. The 'freePBX' logo is on the right. A sidebar on the left lists menu items: 'Básico', 'Gestión de usuarios', 'Extensiones', 'Configuraciones Generales' (highlighted), 'Rutas Salientes', 'Troncales', 'Inbound Call Control', and 'Rutas Entrantes'. The main content area is titled 'Configuración' and contains several sections: 'Opciones de marcado' with input fields for 'Opciones de Marcado' and 'Asterisk Outbound Dial command options'; 'Buzón de Voz' with settings for voicemail duration, prefix, and message type; 'Directorio de la empresa' with a search dropdown and a checkbox for playing extension numbers; 'Maquina de FAX' with settings for fax machine extension and email addresses; 'International Settings' with a dropdown for country indications and a checkbox for 24-hour format; and 'Security Settings' with a checkbox for allowing anonymous inbound SIP calls. A 'Enviar cambios' button is at the bottom. A decorative graphic of colored squares is in the bottom right corner.

Fig. 9 Configuraciones generales

11. En el menú de Configuración elija extensiones para añadir una extensión.



freePBX 2.2.1 on 192.168.1.3 | Configuración | Herramientas | Informes | Panel | Grabaciones | freePBX™

Language: Español Configuración

Básico
Gestión de usuarios
Extensiones
Configuraciones Generales
Rutas Salientes
Troncales
Inbound Call Control
Rutas Entrantes

Añadir una Extensión

Añadir Extensión

Please select your Device below then click Submit

Dispositivo

Dispositivo: Generic SIP Device

Enviar

freePBX 2.2.1 licensed under GPL :: UI Design ©2006 Fischer Design, licensed under Creative Commons

Fig. 10 Añadir extensión

12. Despliegue la pestaña de dispositivo y seleccione Generic SIP Device que es el protocolo que utilizan los softphones. Click en enviar.



Fig. 11 Protocolo de extensión

13. Ingrese el número de extensión, nombre de asociado y el secret. Tanto el número de extensión como el secret deben estar en 200. El nombre de asociado puede ser el de su preferencia pero por comodidad también establézcalo en 200.



Language: Español Configuración

Añadir SIP Extensión

[Añadir Extensión](#)

Añadir Extensiones

Extensión: 200
Nombre asociado: 200

Opciones de la extensión

Direct DID:
DID Alert Info:
CallerID de Salida:
CID de emergencia:

Opciones del dispositivo

This device uses sip technology.
secret: 200
dtmfmode: rfc2833

Fig. 12 Parámetros de las extensiones

14. Para guardar los cambios de click en enviar.
15. De click en Apply Configuration Changes.
16. Agregue 4 extensiones más siguiendo el mismo procedimiento antes descrito.

Actividad 4: Comunicación entre softphones

1. Registre el softphone X-Lite y Zoiper validos en la central Hipath 2000 es decir en la dirección 192.168.1.2.



Fig. 4 X-Lite

2. Para registrar el softphone X-Lite haga click en la pestaña que se muestra en la figura 4, donde aparece Show Menu y luego en la opción SIP Accounts Settings...
3. Haga click en Add nueva cuenta y llene los parámetros tal como se muestra en la figura 5. Tomando como referencia la extensión número 110.
4. El nombre que aparece en el display, el nombre de usuario, la contraseña y la autorización del nombre de usuario se completan introduciendo el número de extensión.
5. El dominio corresponde a la dirección IP de la central Hipath 2000 en este caso.
6. En domain proxy se deja también la misma dirección IP de la central Hipath 2000.

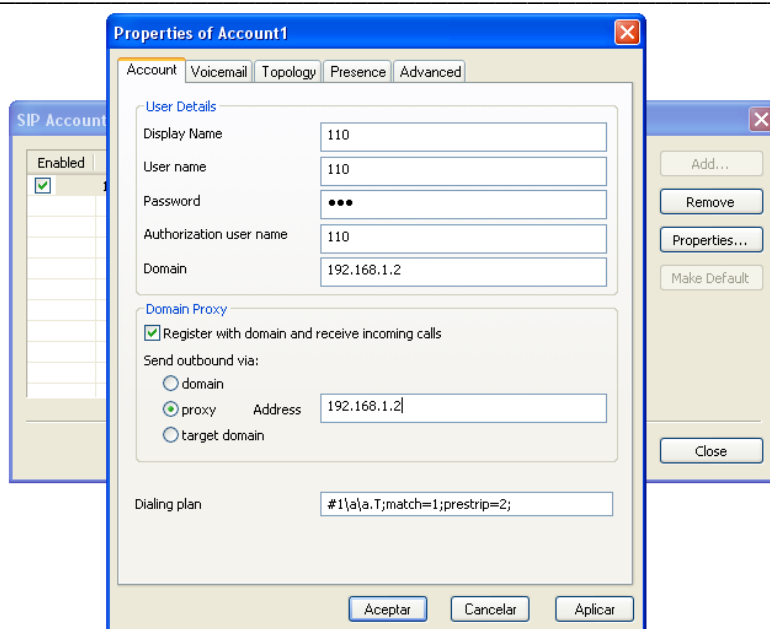


Fig. 5 Propiedades de la cuenta

7. Una vez introducidos todos los datos haga click en Aceptar y cierre la ventana de SIP Accounts en la opción close. Así le aparecerá el número de extensión debidamente registrado en el display del softphone, listo para realizar o recibir una llamada.



Fig. 6 X-Lite registrado

8. De igual manera procedemos ahora a registrar el softphone Zoiper haciendo click en el ícono de Opciones dentro del menú principal.



Fig. 7 Zoiper

9. A continuación se aparecerá una ventana como la que se muestra en la figura 8.
10. Seleccione Cuenta nueva de SIP. Le pedirá el número de la extensión. Introduzca por ejemplo la extensión número 111.
11. Ingrese los datos que aparecen en seguida: El dominio corresponde al número de la dirección IP de la central Hipath 2000, los campos de nombre de usuario, clave y el número de llamante complételo con el número de extensión 111.

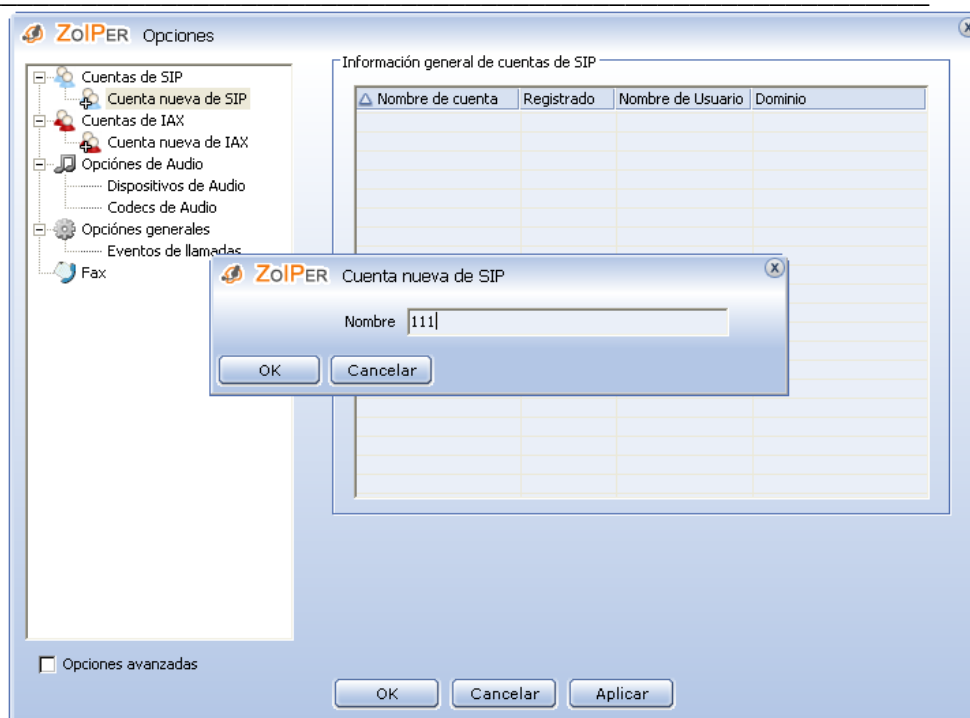


Fig. 8 Cuenta nueva de SIP

12. Una vez introducidos todos los datos haga click en OK para guardar los cambios. Así le aparecerá el número de extensión debidamente registrado en el display del softphone, listo para realizar o recibir una llamada.
13. Para hacer llamadas desde el Zoiper haga click en la viñeta de la parte derecha para desplegar un pequeño teclado para introducir los el número de extensión y luego haga click en Llamar o simplemente introduzca desde el teclado de la computadora el número de extensión y presione Enter.



Fig. 9 Zoiper registrado

14. Para hacer llamadas desde el X-Lite puede presionar los dígitos del teclado del softphone para introducir el número de extensión y luego hacer click en Dial o bien simplemente introduzca desde el teclado de la computadora el número de extensión y presione Enter.
15. Una vez que la llamada esté establecida se observará tal como se muestra en la figura 10.



Fig. 10 Establecimiento de la llamada

Actividad 5: Configuración de adaptador ATA cisco.

Para la configuración de estos adaptadores se seguirán los siguientes pasos:

1. Primero determine la dirección IP que recibió.
 - Para conseguir la dirección IP, levante el teléfono asignado al conector de la línea 1 y Marque: **** (4 asteriscos). Después marque: 110 # y recibirá la dirección IP de su dispositivo (por ejemplo: 192.168.0.100).
2. Use un navegador en su red e ingrese la dirección:
 - **http://<IP ADDRESS>/** (donde <IP ADDRESS> se reemplaza con la dirección que recibió en el paso anterior.



- Haga clic en el botón de "Admin Login" en la esquina superior derecha para iniciar una sesión y después haga clic en la pestaña "Line 1" para seleccionar la línea 1 (Ver Figura 0-1).



Figura 0-1 Configuración adaptador ATA

- Sólo necesitará modificar unos cuantos parámetros establecidos de fábrica. Estos son:

Proxy: Dirección IP del servidor Asterisk

Display Name: Ingrese su nombre completo. El mismo se mostrará como parte de su identificador de llamadas.

User ID: Ingrese el número de extensión que se desea designar según el plan de numeración.

Password: Este es el mismo número de extensión

Register Expires: 3600

Proxy:	<input type="text" value="sip.inphonex.com"/>	Register:	<input type="text" value="yes"/>
Make Call Without Reg:	<input type="text" value="no"/>	Register Expires:	<input type="text" value="3600"/>
Ans Call Without Reg:	<input type="text" value="no"/>		
Display Name:	<input type="text" value="John Doe"/>	User ID:	<input type="text" value="123456"/>
Password:	<input type="text" value="*****"/>	Use Auth ID:	<input type="text" value="no"/>
Auth ID:	<input type="text"/>		

Figura 0-2 Configuración de dirección del servidor Proxy

- Para ahorrar ancho de banda, cambie el Codec de la línea 1 a G729A. También cambie el uso único de Codec "Use Pref Codec Only" a No. Sólo debe hacer esto con una línea. Si la línea 1 está en G.729a, la línea 2 debe estar en otro codec.



Preferred Codec: G729a
Use Pref Codec Only: no
DTMF Tx Method: Auto
Silence Supp Enable: no
FAX CED Detect Enable: yes

- Haga click en el botón de salvar la configuración "Save settings" al final de la página.

Actividad 5: Realice llamadas entre el adaptador ATA y los softphone.

1. Marque las extensiones que han sido asignadas y realice un conversación entre ambos equipos.

VII. Preguntas de control

1. ¿Qué función posee el protocolo IAX2 y ZAP en Asterisk?
2. ¿Cómo se establece una conferencia en Asterisk?
3. ¿Para qué se utiliza el PIN de administrador en una conferencia?



Laboratorio No. 5: Enlace entre Hipath 2000 y Asterisk. *

Modulo	Telefonía IP		
Tipo Práctica	<input type="checkbox"/> Laboratorio <input type="checkbox"/> Simulación		
Unidad Temática			
No Alumnos por práctica	2	Fecha	
Nombre del Profesor			
Nombre(s) de Alumno(s)			
Tiempo estimado		Vo. Bo. Del Profesor	
Comentarios			

Objetivos de la práctica de laboratorio

I. Objetivo general

1. Establecer el enlace entre la PBX Hipath 2000 y el escenario Asterisk.

II. Objetivos específicos

1. Realizar configuraciones de extensiones, troncales, rutas entre otros.
2. Efectuar la comunicación entre la central virtual Asterisk y la centralita Siemens Hipath 2000.

III. Medios a utilizar

- PBX Hipath 2000
- Equipo de cómputo
- Router
- Softphone Zoiper o Xlite
- Java Ultima version

IV. Introducción

Este laboratorio involucra la interconexión de dos plataformas de comunicación de voz de forma flexible y rápida.



Asterisk es una completa central PBX basado en software, bajo el sistema operativo Linux Centos que permite construir aplicaciones de comunicaciones sin incurrir en altos costos.

HiPath 2000 es una central PBX meramente IP propietaria de Siemens que permite el aprovechamiento todas las ventajas de las comunicaciones IP.

El enlace entre la central PBX Hipath 2000 de tipo IP pura y el escenario Asterisk se efectúa a través de la realización de las configuraciones de extensiones, troncales, rutas entre otros que permiten efectuar la comunicación entre la central virtual Asterisk y la centralita Siemens Hipath 2000.

Se utiliza como interfaz de red una red de área local asignándole una dirección estática al Asterisk y utilizando la dirección por defecto que posee la central Hipath 2000 que es 192.168.1.2.

Se crean extensiones SIP en ambas centrales con el objetivo de validarlos en los softphones X-Lite y Zoiper los cuales trabajan con este protocolo. Además que Asterisk trabaja con este protocolo para la interconexión con la central Hipath 2000 al momento de configurar las troncales.

Estas troncales SIP poseen una ruta asignada para fijar las características de la interconexión entre las centrales. El patrón de marcado que se sigue es para Asterisk el -2xx y para la central Hipath 2000 -1xx.

V. Conocimientos previos

- Softphones
- Laboratorio 5: Introducción a Hipath 2000
- Laboratorio 7: Asterisk

VI. Procedimiento

El escenario a implantarse se muestra en la figura 1. Aquí se presenta la interconexión como tal:

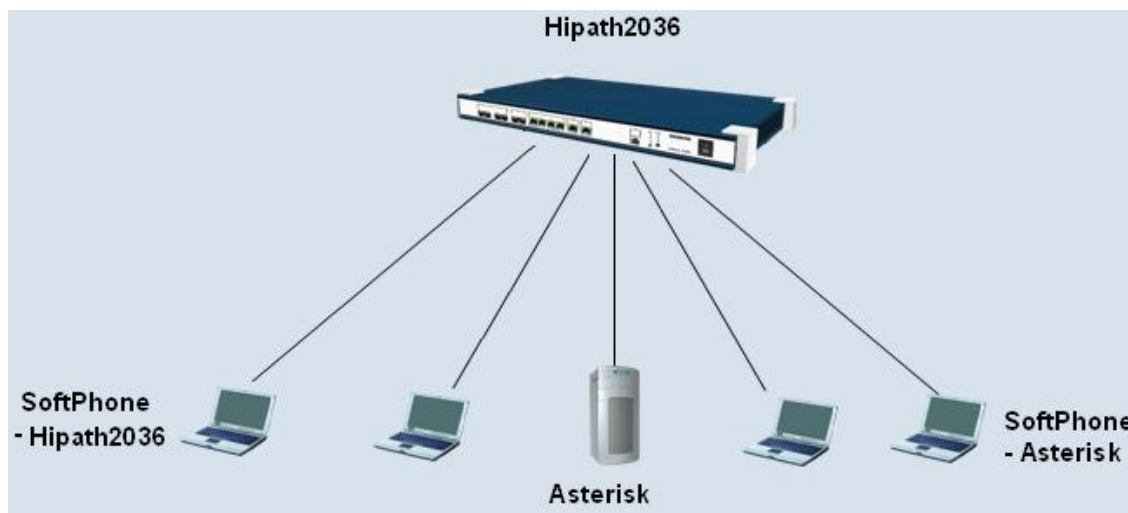


Fig. 1 Escenario del laboratorio.

Ambas centrales PBXs utilizarán softphones que se tratan de software que se ejecuta en estaciones o servidores de trabajo que permiten establecer llamadas de voz sobre IP.

Parte 1

Actividad 1: Configuración de la dirección IP del Asterisk

1. Conecte la centralita Hipath 3000 al suministro eléctrico y oprima el switch de encendido/apagado.
2. Inicialice el Asterisk mediante una máquina virtual.
3. Cuando cargue el sistema operativo Linux Centos aparecerá el login para ingresar al Asterisk y luego el password. El login es root mientras que la contraseña es definida por el usuario. En este caso la contraseña es electrónica.
4. Para salir de Asterisk presione Control + Alt.



```
CentOS release 4.4 (Final)
Kernel 2.6.9-34.0.2.EL on an i686

asterisk1 login: root
Password:

Welcome to trixbox
-----

For access to the trixbox web GUI use this URL
http://192.168.98.128

For help on trixbox commands you can use from this
command shell type help-trixbox.

[root@asterisk1 ~]# _
```

Fig. 2 Asterisk login

- Introduzca el comando netconfig para cambiar la dirección IP que contiene por defecto el Asterisk y presione yes.



Fig. 3 Comando netconfig

- Ingrese los parámetros de configuración IP.
- Establezca la dirección IP en 192.168.1.3; máscara 255.255.255.0 y tanto el Gateway por defecto como el primary nameserver en 192.168.1.1.
- Presione ok.

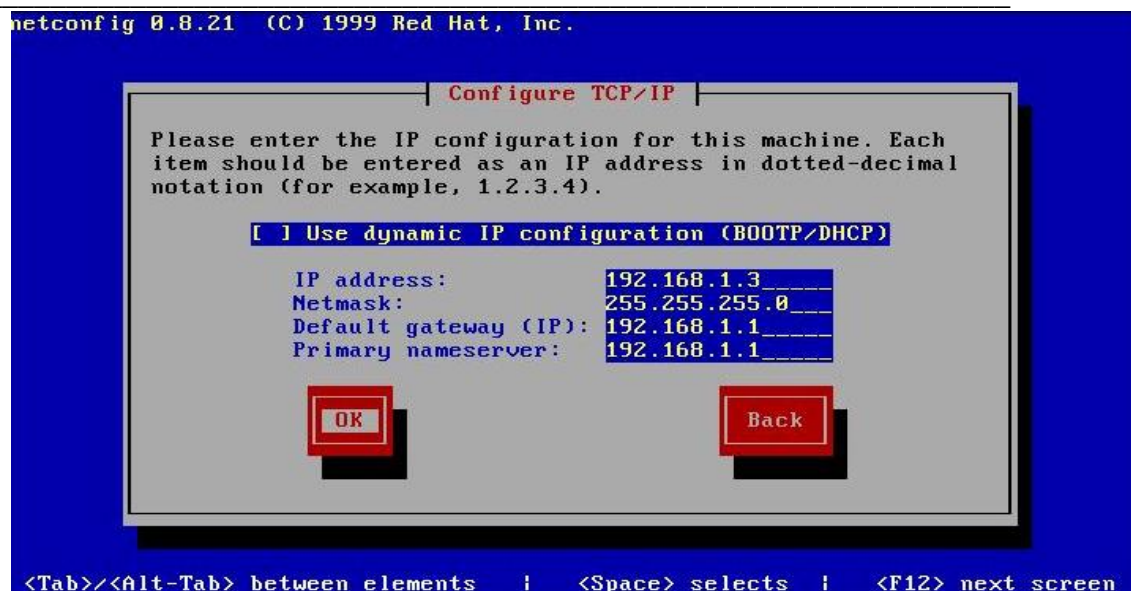


Fig. 4 Configuración TCP/IP

9. Luego escriba el comando `service network restart` para reiniciar el servicio de red.
10. Ingrese el comando `ifconfig` para verificar si la información de los parámetros IP está configurada correctamente.

```
[root@asterisk1 ~]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0C:29:F4:76:E6
          inet addr:192.168.1.3  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fef4:76e6/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:586 errors:0 dropped:0 overruns:0 frame:0
          TX packets:618 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:83133 (81.1 KiB)  TX bytes:166882 (162.9 KiB)
          Interrupt:5 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:148 errors:0 dropped:0 overruns:0 frame:0
          TX packets:148 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:19202 (18.7 KiB)  TX bytes:19202 (18.7 KiB)

[root@asterisk1 ~]# _
```

Fig. 5 Comando ifconfig

Actividad 2: Añadir extensiones en el Asterisk

1. Realice el mismo procedimiento efectuado en la actividad 3 del laboratorio 7 correspondiente a Asterisk.



Actividad 3: Añadir Troncales en el Asterisk

1. En el menú de Configuración elija Troncales.
2. Seleccione agregar una troncal SIP.
3. En la casilla correspondiente a Reglas de Marcado Saliente introduzca 1xx que será el patrón a utilizar en las extensiones de la Hipath 2000.
4. Configure los detalles de las troncales de la salida y de entrada tal como se muestra en la figura 6.
5. De click en enviar.
6. De click en Apply Configuration Changes.

freePBX 2.2.1 on 192.168.1.3 | Configuración | Herramientas | Informes | Panel | Grabaciones | freePBX™

Language: Español Configuración

Básico
Gestión de usuarios
Extensiones
Configuraciones Generales
Rutas Salientes
Troncales
Inbound Call Control
Rutas Entrantes

Add SIP Trunk

Configuraciones Generales

Caller ID Saliente:
Never Override CallerID: ☐
Canales Máximos:

Reglas de Marcado Saliente

Reglas de Marcado:

Asistente de reglas de marcado: (elegir uno)
Prefijo de Marcado Saliente:

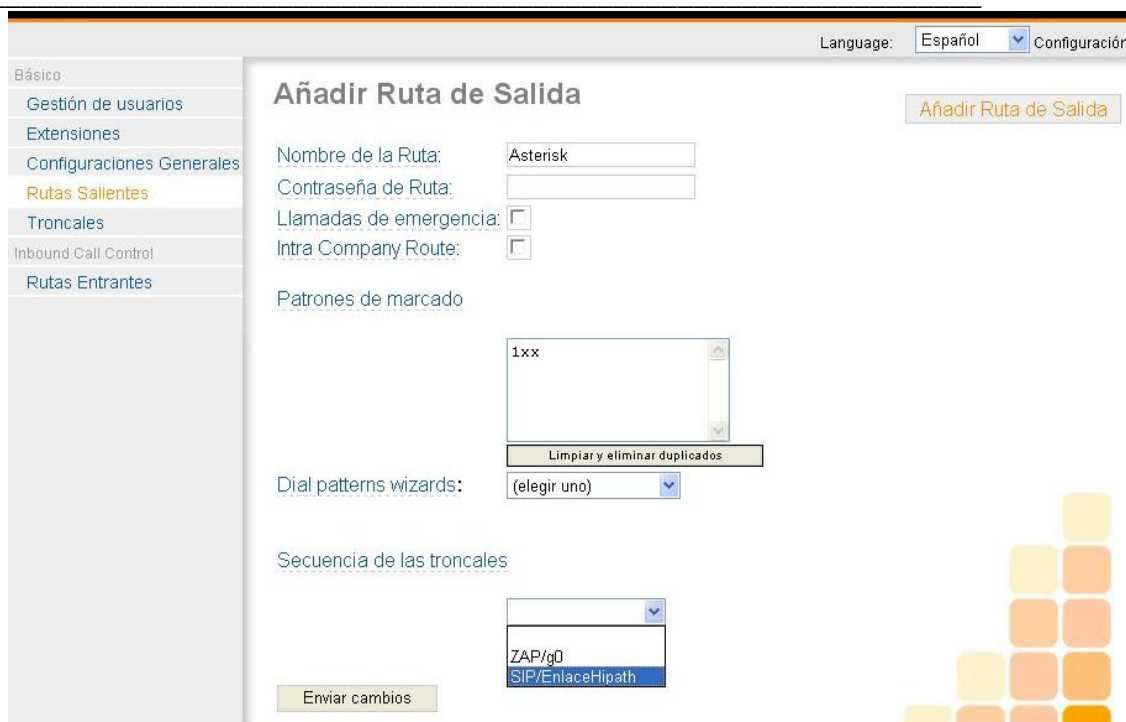


The screenshot displays the Asterisk configuration web interface. On the left is a grey sidebar. The main content area is divided into two sections. The top section, 'Configuración de salida', has a text input for 'Nombre de la Troncal' containing 'EnlaceHipath'. Below it, 'Detalles del troncal de salida:' is followed by a text area containing the following configuration: `canreinvite=yes`, `context=from-internal`, `host=192.168.1.2`, `nat=yes`, `qualify=very`, and `type=friend`. The bottom section, 'Configuración de Entrada', has a text input for 'Contexto del troncal de entrada' containing 'from-internal'. Below it, 'Detalles del troncal de entrada:' is followed by an empty text area. To the right of the configuration area, there are three small colored squares (yellow, orange, and red) arranged in a triangular pattern.

Fig. 6 Configuración de troncales en Asterisk.

Actividad 4: Añadir Ruta de Salida en el Asterisk

1. En el menú de Configuración elija Rutas Salientes.
2. De click en Añadir Ruta de Salida.
3. Ingrese el nombre de la Ruta de Salida "Asterisk".
4. En la casilla correspondiente a Patrones de marcado introduzca 1xx que será el patrón a utilizar en las extensiones de la Hipath 2000.
5. En la casilla correspondiente a Secuencia de las troncales, seleccione la troncal creada SIP/EnlaceHipath.
6. De click en enviar cambios.
7. De click en Apply Configuration Changes



Language: Español Configuración

Añadir Ruta de Salida Añadir Ruta de Salida

Nombre de la Ruta: Asterisk

Contraseña de Ruta:

Llamadas de emergencia: ☐

Intra Company Route: ☐

Patrones de marcado

1xx

Limpiar y eliminar duplicados

Dial patterns wizards: (elegir uno)

Secuencia de las troncales

ZAP/g0

SIP/EnlaceHipath

Enviar cambios

Fig. 7 Configuración de ruta parte 1 en Asterisk.

8. Añada otra Ruta Saliente ahora con el nombre de prueba, tal como lo hizo con la ruta Asterisk.



Language: Configuración

Añadir Ruta de Salida Añadir Ruta de Salida

Nombre de la Ruta: Prueba

Contraseña de Ruta:

Llamadas de emergencia: ☐

Intra Company Route: ☐

Patrones de marcado

1xx

Limpiar y eliminar duplicados

Dial patterns wizards: (elegir uno)

Secuencia de las troncales

SIP/EnlaceHipath

Enviar cambios

0 Asterisk

Fig. 8 Configuración de ruta parte 2 en Asterisk.



9. Ahora observe el patrón de las rutas de salida en la figura 9, una flecha va hacia afuera mientras la otra hacia adentro. Eso significa que la ruta de salida Asterisk fue configurada correctamente como tal.

Fig. 9 Configuración de ruta parte 3 en Asterisk.

Actividad 5: Comunicación entre softphones

1. Realice el mismo procedimiento efectuado en la actividad 4 del laboratorio 5 correspondiente a la Hipath 2000.

Actividad 6: Asignación

1. Investigue en qué consiste cada comando utilizado en los detalles de las troncales de la salida y de entrada.



Parte 2

Actividad 1: Configuraciones de la central Hipath 2000

1. Realice las primeras 4 actividades del laboratorio 5 correspondiente a la Hipath 2000.

Actividad 2: Anadir un nodo en la Hipath 2000

1. En el menú explorador de click en Gateway de voz, aparecerán varias carpetas, llamadas Gateway de voz, Proveedor de servicios de telefonía, Gatekeeper, Parámetro códec destino y PBX
2. De click en la carpeta PBX, se desplegaran dos carpetas una carpeta llamada nodo y otra llamada encaminamiento.
3. De click derecho a la carpeta nodo.
4. Seleccione añadir nodo.
5. Para añadir el nodo te piden el número. Como no hay ningún nodo creado hasta el momento se le puede poner cualquier número, pero como en este laboratorio se hará una interconexión con Asterisk le pondremos un numero 2, ya que las extensiones que se crearon en Asterisk comienzan con este número.
6. De click en asumir.
7. Espere que el menú vuelva a cargar y luego busque PBX.
8. De click en PBX, luego nodo y ahí podrá observar el nodo creado.
9. De click derecho en el nodo creado y seleccione editar direcciones IP. Se desplegara una ventana con los parámetros del nodo creado.
10. En protocolo Lan trunking aparece por defecto H323-Q. Cámbielo por SIP nativo.



11. En módulo HGX-1: Dirección IP se tiene que poner la dirección IP de la central con la cual se desea hacer el enlace. En este caso es la dirección IP en la que se encuentra el Asterisk, la cual es 192.168.1.3
12. En Supervisión de nodos déjelo sin activar.
13. De click en asumir.
14. De click en guardar.

Actividad 3: Configuración del enrutamiento en la Hipath 2000

1. En Gateway de voz, seleccione la carpeta PBX y luego la carpeta encaminamiento.
2. De click derecho en la carpeta encaminamiento, y luego elegir número de llamada. Se desplegará una ventana en donde se selecciona el nodo por donde entrara la llamada y el prefijo de las llamadas que entraran a ese nodo.
3. En número de nodo seleccione el nodo 2 que se creó anteriormente.
4. En número de llamada escriba el número con el cual comienzan las extensiones de la central en la cual se hará el enlace. En este caso es el número 2.
5. En servicio seleccione voz.
6. De click en asumir
7. Guarde los cambios.

Actividad 4: Configuración de códecs

Actividad 4.1: Configuración de los parámetros códecs

1. En Gateway de voz, seleccione la carpeta Gateway de voz.
2. Seleccione parámetros códec y de click derecho editar.
3. Configúrelos tal y como se muestra en la figura 10.
4. De click en asumir.

5. Guarde los cambios.

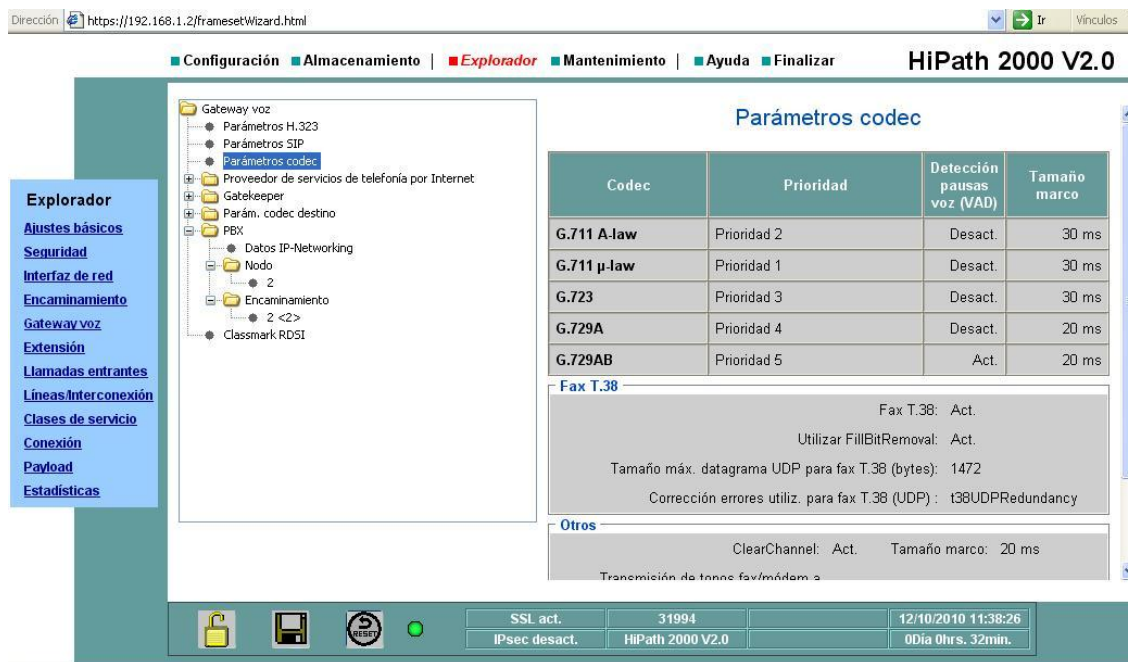


Fig. 10 Configuración de parámetros códec parte 1 en Hipath 2000.

Actividad 4.2: Configuración de los parámetros códec de destino

1. En Gateway de voz, busque la carpeta parámetros códec destino.
2. Seleccione parámetros códec y de click derecho añadir.
3. Configúrelos tal y como se muestra en la figura 11.
4. En tipo de dirección de destino seleccione Host.
5. En dirección IP escriba la dirección de la central con la cual se va a hacer el enlace, en este caso la de Asterisk. 192.168.1.3
6. De click en asumir.
7. Guarde los cambios.

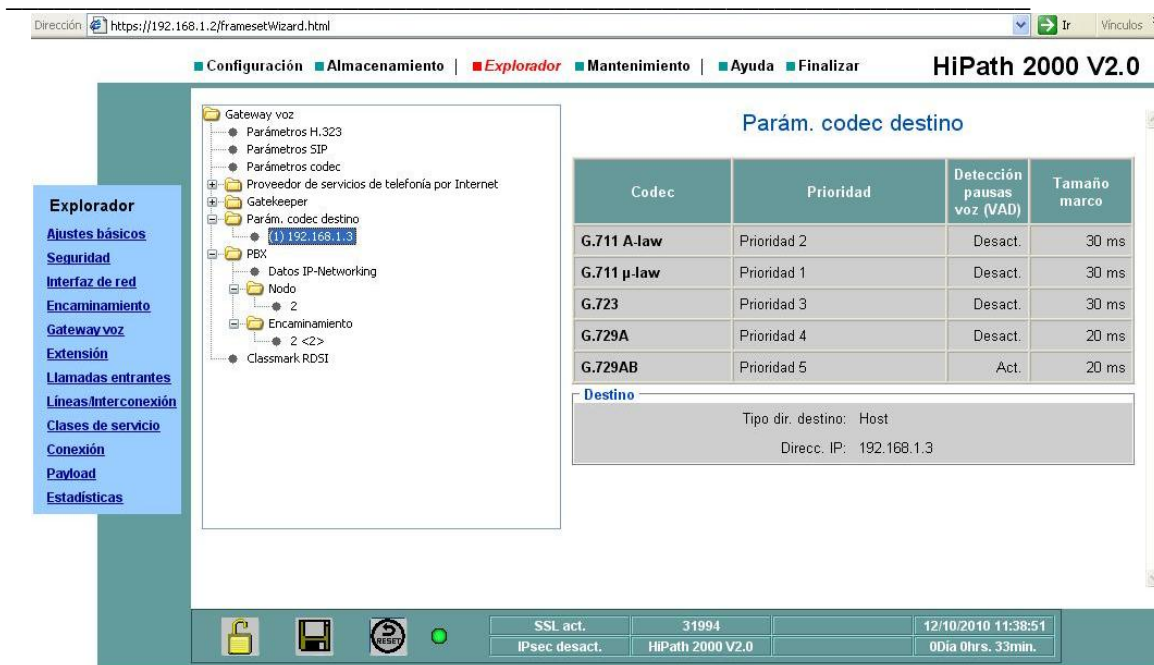


Fig. 11 Configuración de parámetros códec parte 2 en Hipath 2000.

Actividad 5: Configuración de rutas en la Hipath 2000

1. Seleccione la carpeta Rutas.
2. Elija la ruta que desea utilizar para la interconexión con Asterisk.
3. De click derecho cambiar ruta.
4. Cambie el nombre de la ruta y póngale Asterisk
5. De click en asumir.
6. Guarde los cambios.

Actividad 6: Configuración de líneas en la Hipath 2000

1. En el menú explorador, seleccione la carpeta líneas/interconexión, y luego la carpeta correspondiente a Líneas.
2. En la carpeta Líneas se desplegarán dos carpetas una de nombre LAN: Slot 2 y otra de nombre Analog: Slot 4, seleccione LAN: slot 2
3. En LAN: slot 2 se desplegarán varias carpetas, seleccione la carpeta Port 3 Cornet-IP.



4. De click derecho en Port 3 Cornet-IP y seleccione Agregar línea. Le aparece el número de líneas que se desea agregar, elija 1.
5. A continuación se despliega la nueva línea creada que es la 7807 2-3-1. Haga click derecho en dicha línea y seleccione editar línea.
6. En el campo Ruta, seleccione la ruta que se eligió en la actividad 6 de nombre Asterisk.
7. De click en asumir.
8. Guarde los cambios.
9. De click en la carpeta Analog: slot 4
10. De click en Port 1 Línea analógica
11. Seleccione la línea que se encuentra en esta ubicación y de click derecho editar línea.
12. En la parte donde se elige la ruta seleccione ninguno. Esta opción significa que no hay nada conectado a esta ruta.
13. De click en asumir
14. Repita el inciso 11 y 12 con los puertos analógicos del 2 al 6.
15. Cuando haya realizado todos los cambios de click en guardar.

Actividad 7: Configuración de tabla de ruta.

1. En el menú explorador, seleccione encaminamiento.
2. Seleccione la carpeta LCR
3. Diríjase a la carpeta tabla de rutas.
4. Se puede seleccionar cualquier tabla, por ejemplo elija la tabla 8.
5. De click en editar.
6. Modifíquela tal y como se muestra en la figura 12.

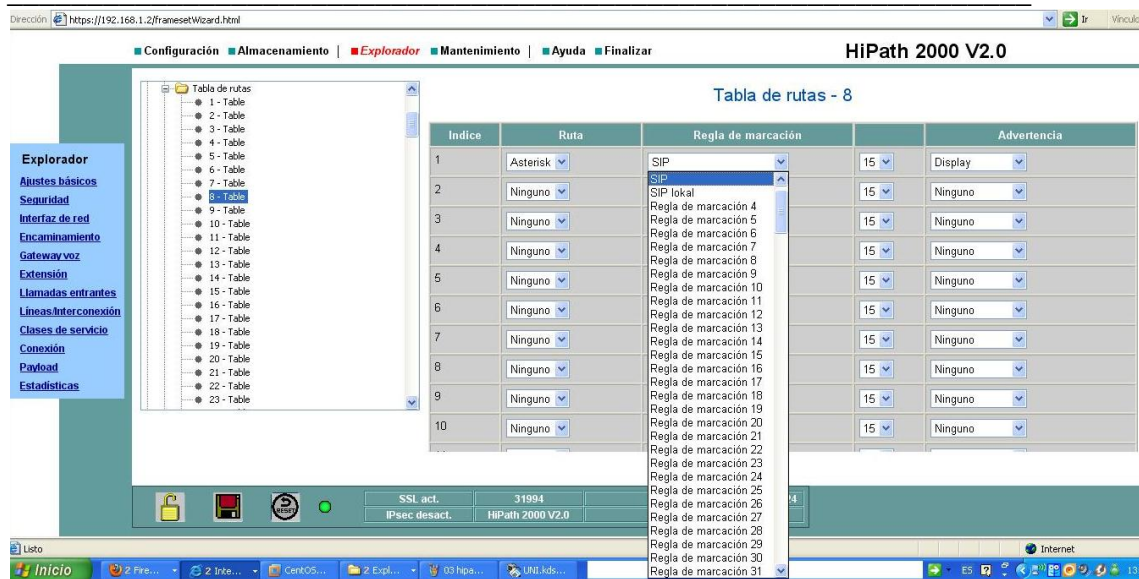


Fig. 12 Configuración tabla de ruta en Hipath 2000.

7. En ruta se selecciona la ruta que se modificó en la actividad 6 de nombre Asterisk.
8. En regla de marcación se elige SIP. Se elige esta opción porque es uno de los protocolos que se utiliza para llamadas de VoIP. SIP ya viene definida en la parte de regla de marcación.
9. De click en asumir.
10. Guarde los cambios.

Actividad 8: Liberación del LCR (Least Cost Routing)

1. En el menú explorador, seleccione encaminamiento.
2. Diríjase a la carpeta LCR.
3. De click derecho editar flags, aparece una ventana como la que se muestra en la figura 13.
4. Modifíquela las opciones tal y como se muestra en la figura 13.
5. De click en asumir.
6. Guarde los cambios realizados.



Fig. 13 Liberación del LCR en Hipath 2000.

Actividad 9: Configuración del plan de marcación

1. En el menú explorador, seleccione la carpeta encaminamiento.
2. Dirijase a la carpeta LCR
3. Seleccione Plan de marcación, de click derecho editar.
4. Aparecerá una tabla con 3 casillas nombre, cifras marcadas y tabla de rutas
5. Modifique solo la primera fila, en la casilla nombre escriba Asterisk.
6. En la casilla cifras marcadas ponga -2xx. El símbolo – indica que se realizara una llamada fuera de la central local. El símbolo x representa que se esperan números del 0-9.
7. En tabla de ruta seleccione la tabla de ruta 8.
8. De click en asumir.
9. Guarde los cambios realizados.



Actividad 10: Verificación de la conexión entre las centrales

1. En el menú explorador, seleccione encaminamiento.
2. Busque la carpeta encaminamiento, se desplegaran varias carpetas seleccione la carpeta Solicitud ICMP.
3. Elija ping, click derecho ejecutar ping
4. En dirección de destino escriba la dirección del Asterisk.
5. De click en enviar.
6. Si la conexión entre las centrales es correcta, aparecen los comandos que se muestran en la figura 14.

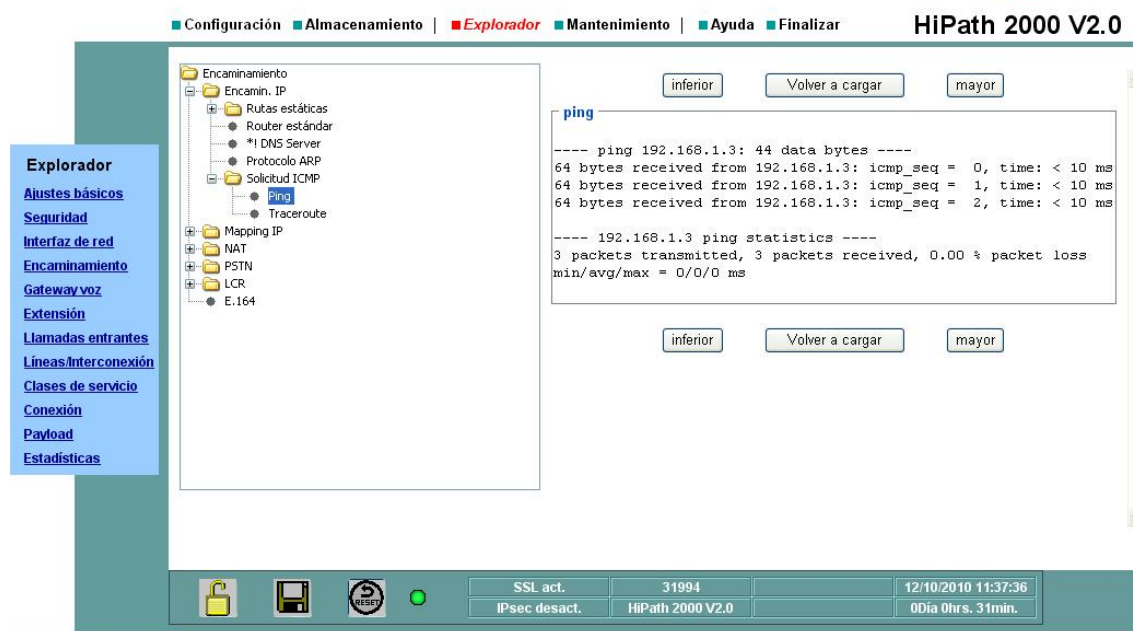


Fig. 14 Verificación de la conexión entre las centrales.

Actividad 11: Comunicación entre softphones

1. Registre el softphone X-Lite en la central Hipath 2000 es decir en la dirección 192.168.1.2.
2. Registre el Zoiper en el Asterisk es decir en la dirección 192.168.1.3.
3. Haga llamadas desde el softphone X-Lite validado en la Hipath 2000 al Zoiper validado en el Asterisk.

4. Haga la operación inversa.



Fig. 15 Zoiper validado en la Hipath 2000 y Sotfphone validados en Asterisk.



Fig. 16 Llamada de la Hipath 2000 a Asterisk.



VII. Preguntas de control

1. ¿Qué es una máquina virtual?
2. ¿Qué es Asterisk?
3. ¿Cuáles son los protocolos que pueden utilizar las extensiones en Asterisk?
4. ¿Cuáles son los códecs de voz que se utilizan en Asterisk?
5. ¿Cuáles son los códecs de voz que se utilizan en la Hipath 2000?



UNIVERSIDAD NACIONAL DE INGENIERÍA
FACULTAD DE ELECTOTECNIA Y COMPUTACIÓN
Departamento de Sistemas Digitales y Telecomunicaciones
Managua, Nicaragua



Laboratorio No. 6: Enlace entre Hipath 2000 y Asterisk sobre monitoreo. *

Modulo	Redes de Telefonía		
Tipo Práctica	<input type="checkbox"/> Laboratorio <input type="checkbox"/> Simulación		
Unidad Temática			
No Alumnos por práctica	2	Fecha	
Nombre del Profesor			
Nombre(s) de Alumno(s)			
Tiempo estimado		Vo. Bo. Del Profesor	
Comentarios			

Objetivos de la práctica de laboratorio

I. Objetivo general

1. Analizar los protocolos que intervienen en el establecimiento de una llamada de VoIP en la central Hipath 2000 y Asterisk.

II. Objetivos específicos

1. Realizar configuraciones de extensiones SIP en la central Hipath 2000.
2. Realizar configuraciones de extensiones SIP en la central Asterisk.
3. Efectuar la interconexión entre las centrales Hipath 2000 y Asterisk.
4. Utilizar la aplicación wireshark 1.2.6 para el análisis de protocolos.

III. Medios a utilizar

- PBX Hipath 2000
- Equipo de cómputo
- Router
- Wireshark
- Softphone Zoiper o Xlite
- Java ultima version



IV. Introducción

Este laboratorio tiene como propósito fundamental explorar de forma práctica el establecimiento de una llamada VoIP mediante el software libre Wireshark 1.2.6. Wireshark captura los paquetes directamente desde una interfaz de red y permite obtener detalladamente la información del protocolo utilizado en el paquete capturado.

Además filtra los paquetes que cumplan con un criterio definido previamente que le permite obtener estadísticas y gráficas.

Estas gráficas permitirán observar detenidamente todo el proceso paso a paso desde que se inicia hasta que finalice la llamada.

Para realizar esta práctica de laboratorio es necesario primeramente entablar el enlace entre estas centrales IP. Una vez efectuada la interconexión se procede a los procesos de captura con Wireshark, un software libre que posee varias funcionalidades para llamadas VoIP.

El proceso de captura se realiza por partes: primero cuando intervienen llamadas desde sólo el servidor Asterisk, luego desde la central Hipath 2000 y finalmente la interconexión entre ambas centrales.

Se analizan los protocolos que intervienen en el establecimiento de una llamada de VoIP en la central Hipath 2000 y Asterisk, así como la señalización que utilizan los protocolos y el registro de llamadas a través de configuraciones de extensiones SIP en ambas centrales.

Con la captura de las llamadas desde el servidor Asterisk es posible incluso escuchar las llamadas haciendo click en el menú Telephony, seleccionando la



opción VoIPCalls y luego en player. Esta funcionalidad sólo está disponible para el tipo de códec G711 A-Law y G711 μ -Law.(Wireshark, 2011)

V. Conocimientos previos

- Softphones
- Laboratorio 5: Introducción a Hipath 2000
- Laboratorio 7: Asterisk
- Laboratorio 8: Enlace entre Hipath 2000 y Asterisk

VI. Procedimiento

Parte 1


Actividad 1: Configuración de extensiones en Asterisk

1. Encienda la máquina virtual para acceder a Asterisk.
2. Siga los pasos de la actividad 3 del laboratorio 7 para añadir 4 extensiones SIP en el Asterisk.
3. Valide dos extensiones en dos softphones distintos.

Actividad 2: Iniciación del Wireshark.

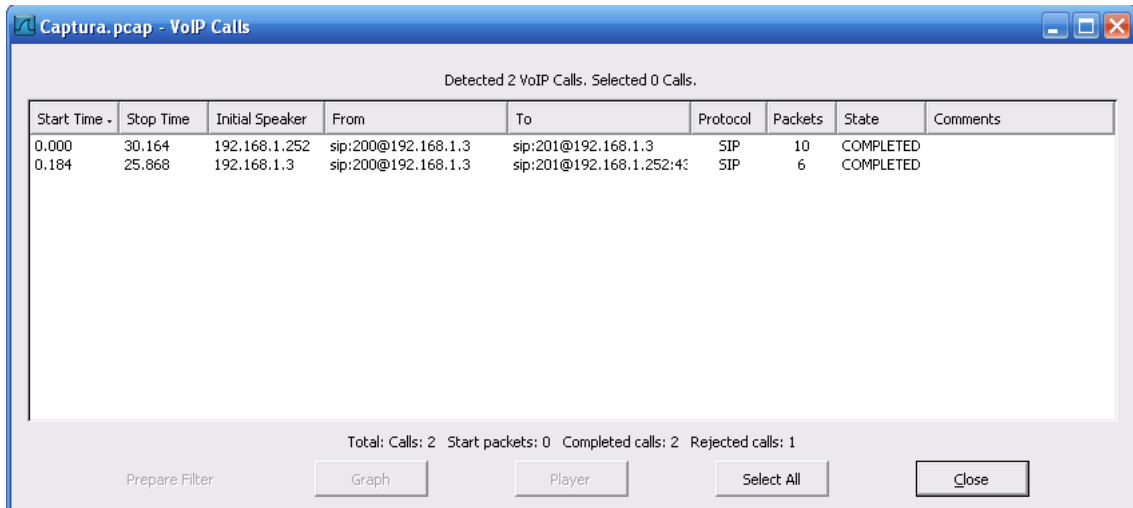
1. Inicie la aplicación Wireshark 1.2.6.
2. En el menú principal haga click en Capture y seleccione Options.
3. En la pestaña Interface, seleccione el adaptador de red que se esté utilizando.
4. Deshabilite Capture packets in promiscuous mode para capturar todos los paquetes detectados por la NIC de la computadora y sólo se dedique a capturar los que llegan meramente a la computadora.
5. Deshabilite Enable transport name resolution por si se distorsiona el análisis que vamos a realizar.

Actividad 3: Proceso de captura de llamadas de Asterisk con Wireshark

1. Haga click en start para empezar el proceso de captura. Diríjase a los softphones antes validados en Asterisk y establezca una conversación por un período de tiempo y luego cuelgue.
2. Ahora detenga el proceso de captura en el wireshark, haciendo click en detener . En el programa se pueden visualizar tres paneles sucesivos donde el panel de arriba es el panel de Lista de cada paquete capturado. Al hacer click en un paquete de este primer panel se logran visualizar los otros dos paneles correspondientes al panel de detalles y de bytes en hexadecimales.
3. Imprima pantalla y guarde la imagen de la captura realizada en su memoria USB.

Actividad 4: Proceso de escuchar la llamada con Wireshark.

1. Para obtener sólo los protocolos correspondientes a SIP coloque en el área de filter SIP y haga click en Apply.
2. Con este resultado haga click en Telephony y seleccione VoIP Calls.



Start Time	Stop Time	Initial Speaker	From	To	Protocol	Packets	State	Comments
0.000	30.164	192.168.1.252	sip:200@192.168.1.3	sip:201@192.168.1.3	SIP	10	COMPLETED	
0.184	25.868	192.168.1.3	sip:200@192.168.1.3	sip:201@192.168.1.252:43	SIP	6	COMPLETED	

Total: Calls: 2 Start packets: 0 Completed calls: 2 Rejected calls: 1

Prepare Filter Graph Player Select All Close

Fig. 1 Tramas capturadas en Asterisk a través de Wireshark

3. Le aparecerá una ventana parecida a la que se muestra en la figura 3.

4. Ambas líneas corresponden a los softphones que intervinieron en la llamada.
5. Seleccione los dos softphones para observar el diagrama de la voz de ambos en una misma ventana y luego haga click en Decode.

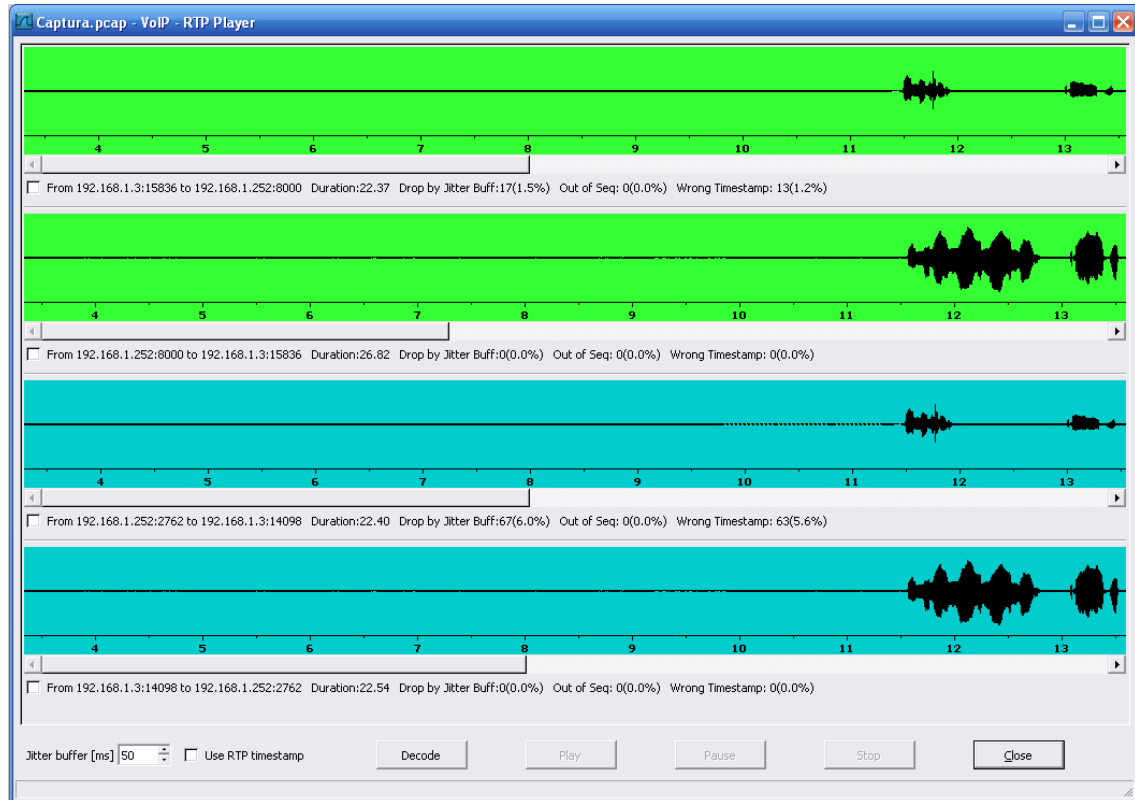


Fig. 2 Grabación de la llamada en Asterisk través de Wireshark

6. Se puede observar que por cada softphone hay dos graficas una correspondiente al micrófono y otra para el audífono. Coloque un check en las verdes y haga click en play para escuchar la llamada.
7. Imprima pantalla y guarde en su memoria USB la imagen de las gráficas correspondientes a la llamada realizada.

Parte 2

Actividad 1: Configuración de extensiones en Hipath 2000

1. Entre a la página de la central Hipath 2000 e introduzca el nombre de usuario y contraseña.



2. Haga click en modo de experto del menú desplegado a la izquierda y elija explorador.
3. Seleccione la opción extensiones y dé click derecho en el primer hipervínculo correspondiente a Extensión.
4. Escoja la opción Editor tablas de extensiones.
5. Configure de 2 a 4 extensiones SIP.
6. Una vez creadas todas las extensiones de click en asumir.
7. Valide dos extensiones en dos softphones distintos.

Actividad 2: Proceso de captura de llamadas de Hipath 2000 con Wireshark.

1. Repita los pasos de la actividad 3 parte 1 del presente laboratorio para capturar la llamada de la Hipath 2000 con Wireshark.

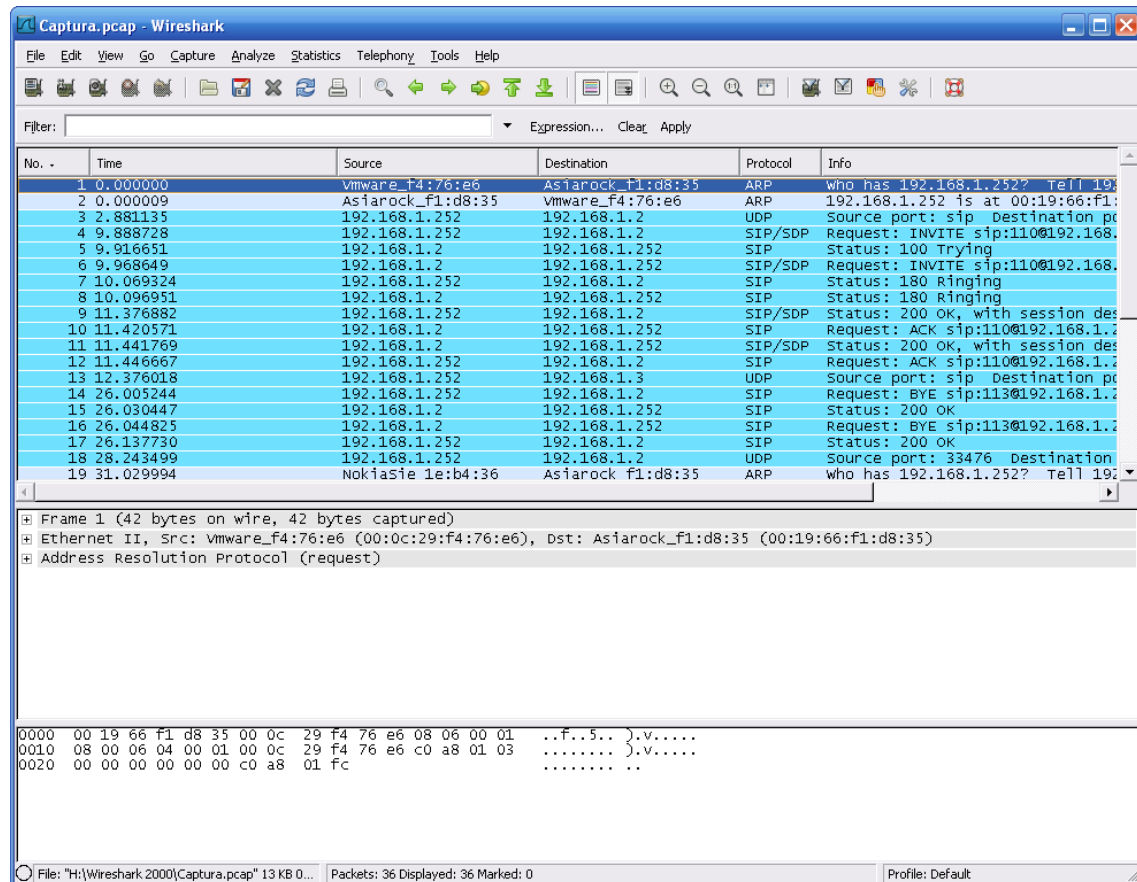



Fig. 3 Tramas capturadas en Hipath 2000 a través de Wireshark

Actividad 3: Diagrama de flujo de llamada.

1. Con los datos capturados en la actividad anterior en el panel de vista se observan cada uno de los paquetes que intervinieron en la captura. Para obtener sólo los protocolos correspondientes a SIP coloque en el área de filter SIP y haga click en Apply.
2. Con este resultado haga click en Statistics y seleccione  Flow Graph...
3. Seleccione Displayed packets para que la gráfica sólo involucre los paquetes que se encuentran dentro del filtro aplicado. De igual manera escoja General flow y Standard source/destination addresses.
4. Pulse Ok para aceptar los parámetros.
5. Imprima pantalla y guarde la imagen su memoria USB correspondiente al diagrama de flujo de la llamada.

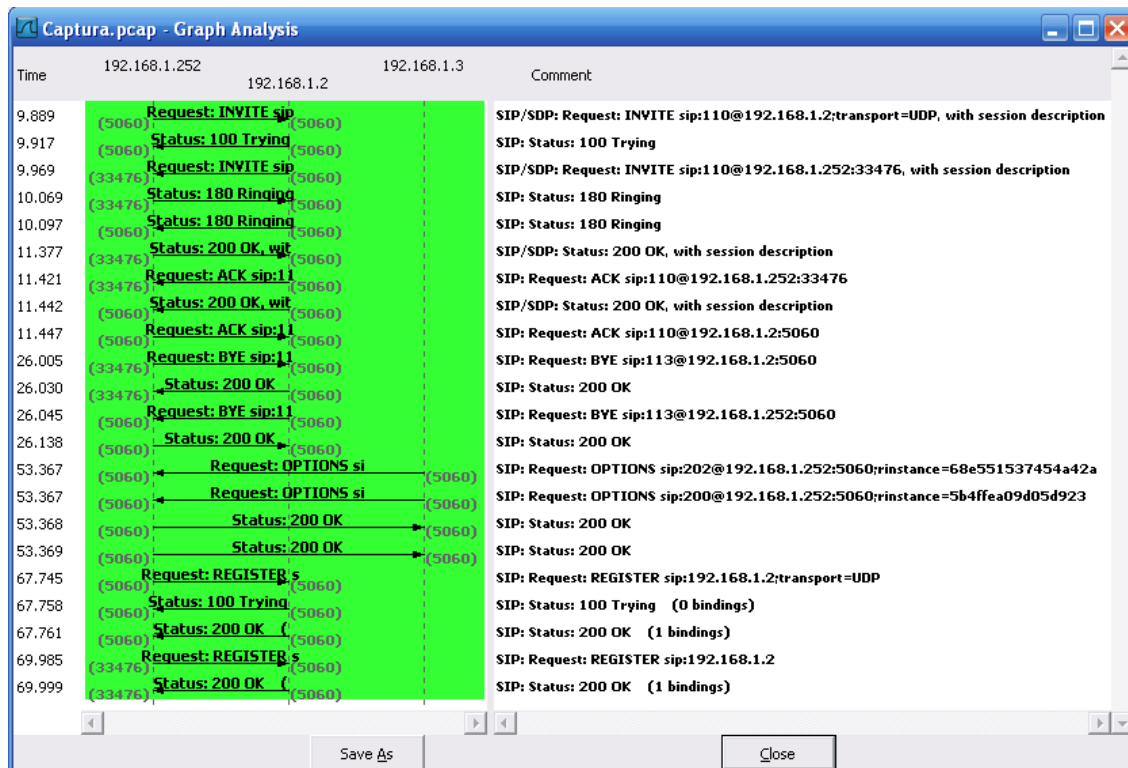


Fig. 4 Diagrama de flujo de llamada en Hipath 2000 a través de Wireshark



Actividad 4: Asignación

1. Valide dos softphones en la hipath 2000 y repita los pasos de la actividad 4 parte uno del presente laboratorio.
2. ¿Cuál es el resultado?
3. ¿A qué se debe esto?

Actividad 5: Captura con Wireshark del enlace Hipath 2000 y Asterisk

1. Establezca el enlace entre la Hipath 2000 y el Asterisk tal como se hizo en el laboratorio anterior.
2. Repita el proceso de captura con Wireshark.
3. Determine el diagrama de flujo de llamada.
4. Repita la actividad 4 parte 1 del presente laboratorio.

VII. Preguntas de control

1. ¿Qué es Wireshark?
2. ¿Por qué cuando se hacen llamadas en Asterisk estas llamadas se pueden escuchar con Wireshark si se capturaron los datos cuando se realizó la llamada y con la Hipath 2000 no se puede?
3. ¿Los mensajes de señalización que se intercambia cuando se inicia el proceso de llamada coinciden con los mensajes de señalización que se estudiaron en clases? Si no es así ¿En que difieren estos mensajes? ¿Las funciones son las mismas? Explique

VIII. Orientaciones del reporte de laboratorio

Adjunte en el reporte de laboratorio todas las imágenes que se guardaron durante esta práctica de laboratorio.

Se deberá seguir el formato de informes de laboratorios. Además se deben presentar las respuestas de las preguntas de control.



IX. Bibliografía

Certain Yance Alfredo, Trixbox al descubierto. © 2006 GECKO EU, GECKO NETWORKS. Todos los derechos reservados. Impreso en Colombia.

<http://profesores.elo.utfsm.cl/~agv/elo323/2s10/projects/FuentealbaDuran/img/manualtrixbox.pdf>

1. Manual de Wireshark



Laboratorio No. 7: Configuración de Call-Center en Asterisk

Modulo	Telefonía IP		
Tipo Práctica	<input type="checkbox"/> Laboratorio <input type="checkbox"/> Simulación	Fecha	
Unidad Temática			
No Alumnos por práctica	2		
Nombre del Profesor			
Nombre(s) de Alumno(s)			
Tiempo estimado		Vo. Bo. Del Profesor	
Comentarios			

Objetivos de la práctica de laboratorio

I. Objetivo general

1. Implementar un sistema de Call-Center utilizando Asterisk

II. Objetivos específicos

1. Explicar el procedimiento para configurar el IVR de Asterisk.
2. Establecer un sistema de colas que logre distribuir las llamadas entrantes al call-center.
3. Configurar las troncales del call-center.

III. Medios a utilizar

- 2 Computadoras
- Audifonos
- Softphone
- Router

IV. Introducción

Un Call Centers” (centros de atención de llamadas) son operados por una compañía proveedora de servicios que se encarga de administrar y proveer soporte y asistencia al consumidor según los productos, servicios o información



necesitada. También se realizan llamadas en función de implementar la venta y cobranzas de la empresa.

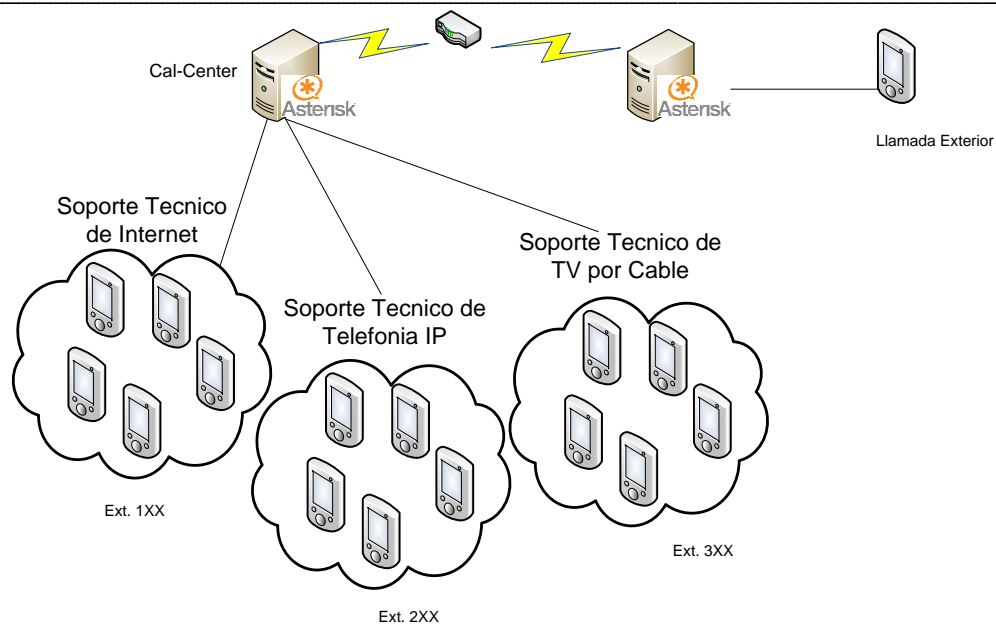
En la actualidad, muchas empresas de call-center deciden evaluar alternativas que les ofrezcan un abaratamiento de costes en su infraestructura con respecto a soluciones tradicionales. Evidentemente, una solución que nos suponga un gran abaratamiento de costes con respecto a soluciones muy establecidas en mercado, como puede ser Avaya, no nos dará todas las funcionalidades que tendríamos con este tipo de infraestructuras, pero sí quizás las suficientes para cubrir todas nuestras necesidades.

Actualmente existen en mercado diferentes soluciones de call-center integrables con Asterisk, que nos darán un entorno de call-center plenamente funcional y con una amplia variedad de funcionalidades, para poner en marcha nuestro negocio.

En este laboratorio se configurara un call-center utilizando los modulos que ofrece Asterisk tales como IVR y sistemas de colas "Queues", los cuales brindan funcionalidades muy adecuadas para creación y buen funcionamiento de un call-center a bajo costo.

V. Procedimiento

El escenario a implantarse se muestra en la figura siguiente. Aquí se presentan los medios a utilizar como son los softphone, PBX virtuales, Router:



Actividad 1: Instalación de PBXs Asterisk

1. Instale dos servidores Asterisk en una PC, cada una de ellas en una máquina virtual.
2. Una vez instaladas y debidamente configurada la tarjeta de red en modo Bridge se configuran las direcciones IP de cada servidor con el comando "netconfig", las direcciones IP serán debidamente distribuidas por el docente.
3. Cuando ya se configure las direcciones IP reiniciamos el servicio de Red con el comando "service network restart".
4. Llamaremos "Asterisk 1" a la PBX que se configurara como Call-Center y "Asterisk 2" a la PBX que simulara la llamada de un usuario solicitando el servicio de "Asterisk 1".

Actividad 2: Instalación de Módulos para configuración de Call-Center

1. Diríjase al explorador web e introduzca la dirección IP de Asterisk 1 para realizar las configuraciones de call-center.



-
2. Cambie a modo Administrador introduciendo el nombre de usuario: maint, y contraseña: password.
 3. Una vez ubicados en modo Administrador, entramos a la opción gestor de módulos ubicada en la parte superior izquierda e instalamos los módulos siguientes:
 - Feature Code Admin
 - Voicemail
 - Phonebook
 - Phonebook Directory
 - Speed Dial Functions
 - Announcements
 - IVR
 - Queues
 - Ring Groups
 - Music on Hold
 - Recordings
 - Call Forward
 - Call Waiting

Actividad 3: Agregar extensiones

1. Agregaremos 9 extensiones para realizar las pruebas de llamadas dentro del call-center, las primeras 5 serán de la extensión 100-102, destinadas al área de soporte técnico de internet, de la extensión 200-202 serán para soporte técnico de Telefonía IP, y de 300-302 para soporte técnico de TV por cable.
2. En la página web nos dirigimos a la opción de configuración y luego a la opción Extensiones ubicado en la parte superior izquierda.



3. Seleccionamos el dispositivo que será Generic SIP Device y seleccionamos la opción Enviar.

freePBX 2.2.1 on 192.168.2.102 | Configuración | Herramientas | Informes | Panel | Grabaciones | freePBX™

Language: Español Configuración

Basic

- Administrators
- Extensions
- General Settings
- Outbound Routes
- Trunks
- Inbound Call Control
- Inbound Routes

Add an Extension

Please select your Device below then click Submit

Device

Device: Generic SIP Device

Submit

freePBX 2.2.1 licensed under GPL :: UI Design ©2006 Fischer Design, licensed under Creative Commons

Add Extension

- 100 <100>
- 101 <101>
- 102 <102>
- 200 <200>
- 201 <201>
- 202 <202>
- 300 <300>
- 301 <301>
- 302 <302>

Actividad 4: Grabación de voz

Existen dos métodos para agregar una grabación, la primera es realizando la grabación a través de uno de los softphone y la segunda simplemente seleccionando un archivo en formato mp3 o wav donde se haya guardado previamente la grabación que deseamos agregar (En caso de ser wav debe ser de 16 bits a 8000Hz).

1. Utilizando el primer método, diríjase a las configuraciones de System Recording, digite el número de extensión de donde realizara la grabación.
2. Asígnele un nombre a su grabación, (ej.: IVR_Bienvenida)
3. Diríjase al softphone y marque *77, luego de escuchar un tono puede empezar su grabación.
4. Para finalizar la grabación solo cuelgue.
5. Marque *99 para escuchar su grabación, si no le gusta la grabación puede grbarla nuevamente marcando *77. (Se recomienda escriba el texto del mensaje para que cuando lo vaya a grabar solo tenga que leerlo). Un ejemplo de Grabacion para el IVR es: "Gracias por llamar a la Empresa de Telecomunicaciones TeleNIC, si conoce el número de extensión dígitelo



ahora, sino marque 1 para comunicarse con soporte técnico de Internet, 2 para Soporte Técnico de Telefonía IP o 3 para Soporte Técnico de TV por cable. Gracias !".

6. Cuando esté satisfecho con su grabación presione guardar en la página web y aplique cambios.

freePBX 2.2.1 on 192.168.2.102 | Configuración | Herramientas | Inf | freePBX™
Grabaciones

Language: Español Configuración

Basic

- Administrators
- Extensions
- General Settings
- Outbound Routes
- Trunks

Inbound Call Control

- Inbound Routes
- Announcements
- IVR
- Queues
- Time Conditions

Internal Options & Configuration

- Music on Hold
- System Recordings**

System Recordings

Add Recording

Step 1: Record or upload

If you wish to make and verify recordings from your phone, please enter your extension number here:

Alternatively, upload a recording in any supported asterisk format. Note that if you're using .wav, (eg, recorded with Microsoft Recorder) the file **must** be PCM Encoded, 16 Bits, at 8000Hz:

No se ha...archivo

Step 2: Name

Name this Recording:

Click "SAVE" when you are satisfied with your recording

7. Realice una nueva grabación, para reproducirla cuando el call-center no logre atender las llamadas solicitadas. Esta puede decir: "En este momento nuestras líneas se encuentran ocupadas, por favor intente su llamada más tarde".

Actividad 5: Configurar Music on Hold

1. Diríjase a configuración - Music on Hold.



2. Agregue una nueva categoría de Music on Hold, designe un nombre, envíe y aplique cambios en la configuración.

freePBX 2.2.1 on 192.168.2.102 | Configuración | Herramientas | Información | Grabaciones

Language: Español Configuración

Basic

- Administrators
- Extensions
- General Settings
- Outbound Routes
- Trunks

Inbound Call Control

- Inbound Routes
- Announcements
- IVR
- Queues
- Time Conditions

Internal Options & Configuration

- Music on Hold
- System Recordings

On Hold Music

Add Music Category

Category Name: mymusic

Submit Changes

Add Music Category

default

3. Seleccione la nueva categoría y agregue el archivo de audio que desea que ese reproduzca mientras se está llamando a una extensión.
4. Presione la opción Upload.
5. Aplique cambios de configuración.



freePBX 2.2.1 on 192.168.2.102 | Configuración | Herramientas | Información | Grabaciones

Apply Configuration Changes Language: Español Configuración

On Hold Music

Category: mymusic

Delete Music Category mymusic

Upload a .wav or .mp3 file:

Seleccionar archivo No se ha seleccionado archivo Upload

Enable Random Play

Completed processing nothin on you Bruno mars .mp3!

nothin on you Bruno mars .mp3 Delete

Actividad 6: configurar sistema de colas

1. En la página web de Asterisk 1 entre al Modulo “Queues” asigne un número y nombre de la cola.
2. Ingrese las extensiones 100,101, 102 en la parte de agentes estáticos, (Esta cola será utilizada para el área de Soporte Tecnico de Internet).



freePBX 2.2.1 on 192.168.2.102

Configuración | Herramientas | Grabaciones

Apply Configuration Changes

Language: Español Configuración

Add Queue

Add Queue

queue number: 1

queue name: servicioInternet

queue password:

CID name prefix:

static agents:

100
101
102

Clean & Remove duplicates

3. En las opciones de colas seleccione la categoría de Music on Hold que anteriormente se agregó.
4. Ponga el tiempo máximo de espera a 2 minutos.
5. Seleccione la estrategia de ring en RONROBIN CON MEMORIA "rrmemory".
6. Después de dos minutos si los teléfonos no se contestan haremos que suene la grabación de Lineas-Ocupadas grabada anteriormente. Seleccione Recordings y escoja Lineas-Ocupadas.



Queue Options

Agent Announcement:

Hold Music Category:

Ring tone instead of MOH: ☐

max wait time:

max callers:

join empty:

leave when empty:

ring strategy:

agent timeout:

retry:

wrap-up-time:

call recording:

event when called:

member status:

Fail Over Destination

☐ IVR:

☐ Phonebook Directory:

☐ Core:

☒ Recordings:

☐ Custom App:

7. Envíe y aplique los cambios.
8. Realice el mismo procedimiento para crear las colas de Soporte Técnico de Telefonía IP (Extensiones 200, 201 y 202), y Soporte Técnico de TV por cable (Extensiones 300,301, 302).

Actividad 7: Configurar IVR

1. Diríjase a las configuraciones de IVR.
2. Agregue un IVR.
3. Elija un nombre para el IVR.



-
4. Elija la grabación que se desea reproducir cuando se ingrese al IVR (IVR_Bienvenida) en la opción Announcement.
 5. En las casillas que aparecen abajo se escribirán los números que se ocuparan para el mensaje de bienvenida, y se asignara hacia que extensiones se desea enviar. En nuestro caso será “1” indicando que es para soporte técnico de internet y se asignara la cola de servicio de internet.
 6. Rellene las casillas para servicio de Telefonía IP y Servicio de TV por cable, así como se muestra en la figura siguiente.



Change Name	<input type="text" value="Bienvenida"/>
Timeout	<input type="text" value="10"/>
Enable Directory	<input checked="" type="checkbox"/>
Directory Context	<input type="text" value=""/>
Enable Direct Dial	<input checked="" type="checkbox"/>
Announcement	<input type="text" value="IVR_Bienvenida"/>

<input type="button" value="Increase Options"/>	<input type="button" value="Save"/>	<input type="button" value="Decrease Options"/>
---	-------------------------------------	---

<input type="radio"/>	IVR: <input type="text" value="Unnamed"/>
<input checked="" type="radio"/>	Queues: <input type="text" value="servicioInternet <1>"/>
<input type="radio"/>	Phonebook Directory: <input type="text" value="Phonebook Directory"/>
<input type="radio"/>	Core: <input type="text" value="Hangup"/>
<input type="radio"/>	Recordings: <input type="text" value="Lineas-Ocupadas"/>
<input type="radio"/>	Custom App: <input type="text" value=""/>

<input type="radio"/>	IVR: <input type="text" value="Unnamed"/>
<input checked="" type="radio"/>	Queues: <input type="text" value="servicioTelefonialP <2>"/>
<input type="radio"/>	Phonebook Directory: <input type="text" value="Phonebook Directory"/>
<input type="radio"/>	Core: <input type="text" value="Hangup"/>
<input type="radio"/>	Recordings: <input type="text" value="Lineas-Ocupadas"/>
<input type="radio"/>	Custom App: <input type="text" value=""/>

<input type="radio"/>	IVR: <input type="text" value="Unnamed"/>
<input checked="" type="radio"/>	Queues: <input type="text" value="servicioTVporCable <3>"/>
<input type="radio"/>	Phonebook Directory: <input type="text" value="Phonebook Directory"/>
<input type="radio"/>	Core: <input type="text" value="Hangup"/>
<input type="radio"/>	Recordings: <input type="text" value="Lineas-Ocupadas"/>
<input type="radio"/>	Custom App: <input type="text" value=""/>

- Agregue dos casillas más presionando la opción de “Increase Options”.
- En estas casillas se agregara la extensión destino “t”, con esta extensión cuando no se presiona ninguna extensión cuando se llama al IVR, las llamadas podrán ser contestadas por una extensión determinada o se podrán enviar al destino que se desee. En nuestro caso la enviaremos a la grabación de Bienvenida.
- Agregue la extensión “i”, la cual contestara las llamadas para las opciones invalidas marcadas en el IVR al momento de llamar, ver figura siguiente



Return to IVR ☐ t

IVR: Bienvenida

Queues: servicioInternet <1>

Phonebook Directory: Phonebook Directory

Core: Hangup

Recordings: Lineas-Ocupadas

Custom App:

Return to IVR ☐ i

IVR: Bienvenida

Queues: servicioInternet <1>

Phonebook Directory: Phonebook Directory

Core: Hangup

Recordings: Lineas-Ocupadas

Custom App:

Increase Options Save Decrease Options

10. Guarde y aplique cambios.

Actividad 8: Configurar Troncales

1. Diríjase a configuración de TRUNKS de Asterisk1 (Call-center).
2. Agregue una Troncal SIP
3. Escriba el nombre que se desee que se muestre cuando se llama desde esta troncal (Call-center).
4. Como el call-center solo recibirá llamadas, no será necesario escribir la regla de marcado.
5. Diríjase a las configuraciones salientes.
6. Escriba el nombre de la troncal (Asterisk2, para hacer referencia a la PBX que se va a conectar).
7. Configure el campo "PEER Details" de la misma manera como se muestra en la figura siguiente, a excepción del host, la dirección IP que escribiremos en el host será la dirección IP que designamos a Asterisk2.
8. El username indica el número principal de la PBX.



Outgoing Settings

Trunk Name:

PEER Details:

```
canreinvite=yes  
context=from-trunk  
host=192.168.2.100  
nat=yes  
qualify=very  
type=friend  
username=1800
```

Incoming Settings

USER Context:

USER Details:

9. Guarde y aplique cambios.
10. Diríjase a la página web de Asterisk 2.
11. Entre a configuración de TRUNKS de Asterisk2
12. Cree una troncal y realice las configuraciones de la troncal del mismo modo que se hizo con Asterisk 1, con la diferencia que en la regla de marcado pondremos el número principal de Asterisk 1 (1800).
13. En la parte de “PEER Details” el host será la dirección IP del call-center “Asterisk1”, y el username será 1801, ver figura siguiente.



Outbound
Caller ID:

Never
Override ☐

CallerID:

Maximum
channels:

Outgoing Dial Rules

Dial
Rules:

Dial rules
wizards:

Outbound
Dial
Prefix:

Outgoing Settings

Trunk
Name:

PEER Details:

```
canreinvite=yes
context=from-trunk
host=192.168.2.102
nat=yes
qualify=very
type=friend
username=1801
```

14. Guarde y aplique cambios.

Actividad 9: Configurar Rutas salientes

1. Diríjase a configuración de rutas saliente en Asterisk2.
2. Agregue una nueva ruta.
3. Asígnele un nombre.
4. En las reglas de marcado ponga 1800.
5. Elija la Troncal que se creó anteriormente.



Add Route

Route Name:

Route Password:

Emergency Dialing: ☐

Intra Company Route: ☐

Dial Patterns

Clean & Remove duplicates

Dial patterns wizards:

Trunk Sequence

Submit Changes

6. Envíe cambios y aplique configuraciones.

Actividad 10: Configurar Rutas entrantes

1. Diríjase a la apágina web de Asterisk 1.
2. Entre a configuraciones de Rutas entrantes.
3. Configure la destinación de la ruta entrante en la opción IVR, y seleccione la grabación de bienvenida que se hizo para la IVR. Ver figura



☒ IVR:

☐ Queues:

☐ Phonebook Directory:

☐ Core:

☐ Recordings:

☐ Custom App:

4. Guarde y aplique cambios.

Actividad 11: Realizar llamadas

1. Con los sftphone registrados en Asterisk 2 marque el número del call-center 1800.
2. Cuando marque la opción 1, observe el orden en que suenan los teléfonos 100, 101,102.
3. Deje repicar los teléfonos por más de 2 minutos.
4. Registre los softphone en las extenciones 200, 201, 202.
5. Marque nuevamente el número del call-center 1800.
6. Observe el orden de las llamadas.

VI. Preguntas de control

1. ¿Qué es el IVR?
2. ¿En qué consiste el algoritmo RonRobin con memoria?
3. ¿Cuál número se debe de marcar para realizar una grabación?
4. ¿Con cuál número se simula una llamada entrante?
5. ¿Qué es y en que consiste un sistema de colas?
6. ¿Para que sirven las extenciones “t” e “i” en la IVR?



Laboratorio No. 8: Interconexión de centrales Asterisk a través de red MPLS.

Curso	Capacitación en telefonía IP		
Modulo	Redes de Datos	Grupo	
Tipo Practica	<input type="checkbox"/> Laboratorio	<input type="checkbox"/> Simulación	
Unidad Temática			
No Alumnos por practica	1	Fecha	
Nombre del Profesor			
Nombre(s) del Alumno(s)			
Tiempo estimado	180 minutos	Vo. Bo. Del Docente	
Comentarios			

Objetivos de la práctica de laboratorio

I. Objetivo General

1. Configurar una red MPLS y realizar llamadas IP a través de ella. .

II. Objetivos específicos

1. Mostrar los comandos para establecer el funcionamiento del protocolo LDP.
2. Configurar el protocolo de enrutamiento dinámico OSPF.
3. Establecer llamadas a través de la red MPLS.

III. Medios a utilizar

- Equipo de computo
- Router cisco 2800
- Plataforma de máquina virtual VMWare
- Central virtual PBX Asterisk
- Softphones.
- Switch Catalyst 2960

IV. Introducción

El laboratorio a implementar pretende simular la red de MPLS un ISP y la comunicación entre centrales virtuales asterisk. Este puede ser el caso de una

empresa que tiene distintas sucursales en el mundo y debe establecer comunicación entre las distintas partes.

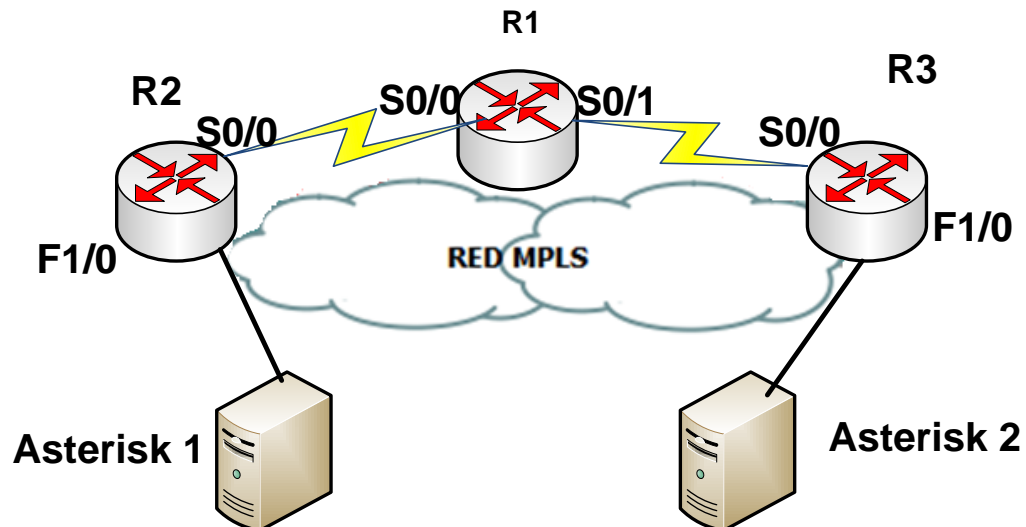
El laboratorio expone los componentes o paquetes de la red MPLS en el proceso de transmisión de paquetes entre centrales telefónicas.

V. Conocimientos previos

- Protocolos OSPF.
- Programación básica de interfaces seriales.
- Configuración de protocolo OSPF en redes IP
- Funcionamiento de redes MPLS.
- Configuración de troncales en centrales Asterisk.

VI. Procedimiento

Actividad 1. Configuración de la red MPLS del ISP.



Dispositivo	Puerto	Dirección IP	Mascara de red
R2	Fa 1/0	10.0.0.2	Clase C
R2	S 0/0	10.0.1.1	Clase C



R1	S 0/0	10.0.1.2	Clase C
R1	S 0/1	10.0.2.1	Clase C
R3	S 0/0	10.0.2.2	Clase C
R3	Fa 1/0	10.0.3.1	Clase C

Paso 1. Interconecte los dispositivos según muestra la figura anterior.

Los router a utilizar son los C2811. Recuerde que los enlaces entre los router R1 y R3 son seriales, en cambio el enlace entre R1 y R2 a través del switch es Ethernet. Y al momento de conectarlos debe utilizar el cable DCE iniciado en R1 hacia R3 para que se reconozca que este será el DCE.

Paso 2. Proceda a asignar las direcciones IP a las terminales de los dispositivos, según se muestran en la tabla de referencia.

Paso 3. Configure la terminal DCE del router R1 con un clock rate de 64000.

Paso 4. Verifique que las terminales entre R1 y R3 están conectadas y existe comunicación entre ellas enviando mensajes ICMP entre los puntos conectados directamente.

Ingresa a la línea de comando de cada router y utilice el comando ping. En este punto la red solo debe ser capaz de enviar y recibir mensajes ICMP entre nodos adyacentes.

Actividad 2. Configuración de la interfaz loopback en los routers
La interfaz loopback sirve como un identificador para el router en que se configura.



Hacemos énfasis en configurarle porque es necesaria para la configuración del protocolo OSPF que se configuraran más adelante, pues se asocia la interfaz loopback a procesos en OSPF.

Las sesiones OSPF requieren de la existencia de una interfaz, en caso de asociarlo a una interfaz física, se corre el riesgo que esta se dañe y se pierda la conexión. Por ende se prefiere asociar los procesos a una interfaz virtual.

Paso 1. Para configurarle se utilizan los comandos:

R1# configure terminal

R1(config)# interface loopback 0

R1(config)# ip address 192.168.1.1 255.255.255.0

Solamente los router R1, R2 y R3 se configuraran con las interfaces loopback. Las interfaces pueden denotarse por cualquier número; en este caso, le llamamos 0. Las direcciones IP de las interfaces loopback deben ser distintas entre los router pero deben pertenecer todas a la misma red. Es decir, a la red 192.168.1.0.

Paso 2. Realice el proceso del paso 1 para los router R2 y R3, asignados diferentes direcciones IP.

Paso 3. Verificación de las interfaces loopback

Verifique que las interfaces loopback se han configurado correctamente en cada router utilizando el comando

R1# show ip interface brief



Actividad 3. Configuración OSPF

Paso 1. Para configurar el protocolo OSPF seguiremos el procedimiento desarrollado en el laboratorio 9 del módulo II.

Los comandos son:

R1# configure terminal

R1(config)# router ospf 1

R1(config – router)# network 10.0.0.0 0.0.0.255 area 1

R1(config – router)# network 10.0.1.0 0.0.0.255 area 0

R1(config –router)#^Z

En este caso, se han definido 3 áreas OSPF. Las área 1 y 2 corresponden a las secciones fuera de la red MPLS y el área 0 es el backbone de MPLS.

Paso 2. Realice el mismo procedimiento para los router R2 y R3.

Paso 4. Revise que la configuración del protocolo OSPF es correcta a través de los comandos:

R1# s hip ospf interface

R1# s hip opsf neighbors

Paso 5. Verifique que existe conectividad entre los router no adyacentes enviando mensajes ICMP entre los routers no adyacentes de la red MPLS y finalmente entre las router R4 y R5.

Actividad 4. Configuración básica de MPLS.

El escenario para establecer el protocolo MPLS ya está listo, ahora es necesario iniciar el protocolo de distribución de etiquetas en las distintas interfaces en las que se desea se transmita a través de etiquetas.



Paso 1. Configure el reenvío express de cisco en todos los router que tienen funcionalidad PE y P. CEF es el conjunto de funcionalidades que reúnen los equipos CISCO para poder trabajar en un entorno MPLS en otras funciones.

Los comandos a utilizar son:

R1# configure terminal

R1(config)# ip cef

Para comprobar que el CEF ha sido activado en el router es necesario utilizar el comando ***sh ip cef summary***. Si está activado nos mostrara una tabla sobre los comandos hábiles en el router. Algo importante es la versión de esta tabla, algunas tablas pueden activarse pero si la versión no es tan reciente puede que el router no reconozca algunos comandos de MPLS.

Paso 2. Este mismo proceso se debe llevar a cabo en los router R2 y R3.

Paso 3. Activación del protocolo de distribución de etiquetas LDP.

En esta parte designaremos que interfaces redirigen mediante el protocolo MPLS. Note que solamente las interfaces seriales de los routers utilizaran MPLS.

Los comandos a utilizar son:

R1 (config)# interface s0/0

R1 (config – if)# mpls ip

R1 (config – if)# mpls label protocol ldp

R1 (config – if)# exit

R1 (config)# interface s0/1

R1 (config –if)#mpls ip



R1 (config – if)mpls label protocol ldp

Paso 4. Realice el mismo proceso para las interfaces seriales de los router R2 y R3.

Paso 5. Verifique que los parámetros e interfaces mpls han sido configurados correctamente, usando los comandos:

R1# show mpls interfaces

R1# show mpls ldp parameters

Actividad 5. Configuración de centrales virtuales PBX

1. Inicialice el Asterisk mediante una máquina virtual.
2. Cuando cargue el sistema operativo Linux Centos aparecerá el login para ingresar al Asterisk y luego el password. El login es root mientras que la contraseña es definida por el usuario. En este caso la contraseña es electrónica.
3. Para salir de Asterisk presione Control + Alt.

```
CentOS release 4.4 (Final)
Kernel 2.6.9-34.0.2.EL on an i686

asterisk1 login: root
Password:

Welcome to trixbox
-----

For access to the trixbox web GUI use this URL
http://192.168.98.128

For help on trixbox commands you can use from this
command shell type help-trixbox.

[root@asterisk1 ~]# _
```

Fig. 2 Asterisk login

4. Introduzca el comando netconfig para cambiar la dirección IP que contiene por defecto el Asterisk y presione yes.



Fig. 3 Comando netconfig

5. Ingrese los parámetros de configuración IP.
6. Establezca la dirección IP en 192.168.1.3; máscara 255.255.255.0 y tanto el Gateway por defecto como el primary nameserver en 192.168.1.1.
7. Presione ok.





Fig. 4 Configuración TCP/IP

8. Luego escriba el comando `service network restart` para reiniciar el servicio de red.
9. Ingrese el comando `ifconfig` para verificar si la información de los parámetros IP está configurada correctamente.

```
[root@asterisk1 ~]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0C:29:F4:76:E6
          inet addr:192.168.1.3  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fef4:76e6/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:586 errors:0 dropped:0 overruns:0 frame:0
          TX packets:618 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:83133 (81.1 KiB)  TX bytes:166882 (162.9 KiB)
          Interrupt:5 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:148 errors:0 dropped:0 overruns:0 frame:0
          TX packets:148 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:19202 (18.7 KiB)  TX bytes:19202 (18.7 KiB)

[root@asterisk1 ~]# _
```

Fig. 5 Comando ifconfig

Actividad 6. Agregar extensiones

4. Agregaremos 9 extensiones para realizar las pruebas de llamadas dentro del Asterisk 1. Las extensiones serán 2xxx para Asterisk1 y 1xx para Asterisk 2
5. En la página web nos dirigimos a la opción de configuración y luego a la opción Extensiones ubicado en la parte superior izquierda.
6. Seleccionamos el dispositivo que será Generic SIP Device y seleccionamos la opción Enviar.

Actividad 7: Añadir Troncales en el Asterisk1

7. En el menú de Configuración elija Troncales.
8. Seleccione agregar una troncal SIP.
9. En la casilla correspondiente a Reglas de Marcado Saliente introduzca 1xx que será el patrón a utilizar en las extensiones del Asterisk 2



10. Configure los detalles de las troncales de la salida y de entrada tal como se muestra en la figura 6.

11. De click en enviar.

12. De click en Apply Configuration Changes.

The screenshot shows the 'Add SIP Trunk' configuration page in the freePBX 2.2.1 web interface. The page is in Spanish and includes the following sections:

- Configuraciones Generales**
 - Caller ID Saliente: [Text input field]
 - Never Override CallerID: ☐
 - Canales Máximos: [Text input field]
- Reglas de Marcado Saliente**
 - Reglas de Marcado: [Text area containing '1xx']
 - Limpiar y eliminar duplicados: [Button]
 - Asistente de reglas de marcado: [Dropdown menu with '(elegir uno)']
 - Prefijo de Marcado Saliente: [Text input field]
- Configuración de salida**
 - Nombre de la Troncal: [Text input field containing 'EnlaceHipath']
 - Detalles del troncal de salida: [Text area containing 'canreinvite=yes', 'context=from-internal', 'host=192.168.1.2', 'nat=yes', 'qualify=very', 'type=friend']
- Configuración de Entrada**
 - Contexto del troncal de entrada: [Text input field containing 'from-internal']
 - Detalles del troncal de entrada: [Text area]

Buttons for 'Añadir Troncal' and 'Troncal ZAP/g0' are visible in the top right corner.

Fig. 6 Configuración de troncales en Asterisk.

Actividad 8: Añadir Ruta de Salida en el Asterisk1

1. En el menú de Configuración elija Rutas Salientes.
2. De click en Añadir Ruta de Salida.
3. Ingrese el nombre de la Ruta de Salida “Asterisk”.
4. En la casilla correspondiente a Patrones de marcado introduzca 1xx que será el patrón a utilizar en las extensiones del Asterisk2
5. En la casilla correspondiente a Secuencia de las troncales, seleccione la troncal creada Asterisk1/Asterisk2
6. De click en enviar cambios.
7. De click en Apply Configuration Changes

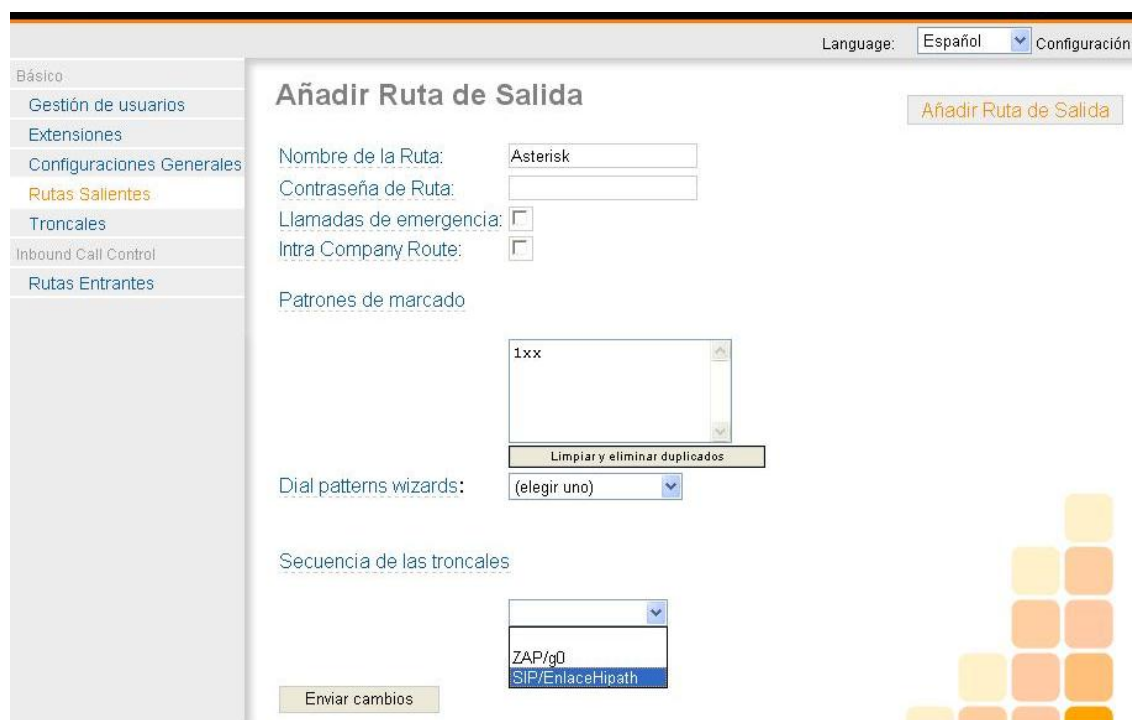


Fig. 7 Configuración de ruta parte 1 en Asterisk.

8. Añada otra Ruta Saliente ahora con el nombre de prueba, tal como lo hizo con la ruta Asterisk1.



The screenshot shows the Asterisk configuration web interface. On the left is a sidebar menu with options: Básico, Gestión de usuarios, Extensiones, Configuraciones Generales, **Rutas Salientes** (highlighted in orange), Troncales, Inbound Call Control, and Rutas Entrantes. The main content area is titled 'Añadir Ruta de Salida'. It contains several input fields: 'Nombre de la Ruta:' with the value 'Prueba', 'Contraseña de Ruta:', 'Llamadas de emergencia:' with a checked checkbox, and 'Intra Company Route:' with a checked checkbox. Below these is a 'Patrones de marcado' section with a text area containing '1xx' and a 'Limpiar y eliminar duplicados' button. Further down is a 'Dial patterns wizards:' section with a dropdown menu showing '(elegir uno)'. The 'Secuencia de las troncales' section has two dropdown menus, the first showing 'SIP/EnlaceHipath'. At the bottom left is an 'Enviar cambios' button. On the right side of the main area, there is a box with 'Añadir Ruta de Salida' and '0 Asterisk'. In the bottom right corner, there is a decorative graphic of a staircase made of orange and yellow squares.

Fig. 8 Configuración de ruta parte 2 en Asterisk.

9. Ahora observe el patrón de las rutas de salida en la figura 9, una flecha va hacia afuera mientras la otra hacia adentro. Eso significa que la ruta de salida Asterisk fue configurada correctamente como tal.



Fig. 9 Configuración de ruta parte 3 en Asterisk.

Realice el mismo proceso de configuración para el Asterisk1.

Actividad 9. Verificación de funcionamiento.

Paso 1. Una vez configurados los terminales Asterisk utilice el comando Ping para verificar conectividad entre los extremos.

Paso2. Proceda a realizar una llamada entre las centrales.

VII. Preguntas de control

Explique el proceso de comunicación de este escenario.